National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
01 – 15 Jul 2024 Vol. 11 No. 13
https://nciipc.gov.in/

Table of Content

Vendor	Product	Page Number
Qualcomm	snapdragon_695_5g_mobile_platform	979
	snapdragon_710_mobile_platform	980
	snapdragon_712_mobile_platform	981
	snapdragon_720g_mobile_platform	982
	snapdragon_750g_5g_mobile_platform	983
	snapdragon_778g_5g_mobile_platform	984
	snapdragon_780g_5g_mobile_platform	985
	snapdragon_7c\+_gen_3_compute	986
	snapdragon_820_automotive_platform	988
	snapdragon_820_mobile_platform	988
	snapdragon_821_mobile_platform	989
	snapdragon_835_mobile_pc_platform	989
	snapdragon_845_mobile_platform	990
	snapdragon_850_mobile_compute_platform	991
	snapdragon_855_mobile_platform	991
	snapdragon_865_5g_mobile_platform	993
	snapdragon_888_5g_mobile_platform	994
	snapdragon_8\+_gen_1_mobile_platform	995
	snapdragon_8\+_gen_2_mobile_platform	997
	snapdragon_8_gen_1_mobile_platform	999
	snapdragon_8_gen_2_mobile_platform	1000
	snapdragon_8_gen_3_mobile_platform	1002
	snapdragon_ar2_gen_1_platform	1004
	snapdragon_auto_4g_modem	1005
	snapdragon_auto_5g_modem-rf	1006
	snapdragon_auto_5g_modem-rf_gen_2	1007
	snapdragon_w5\+_gen_1_wearable_platform	1008
	snapdragon_wear_1300_platform	1009
	snapdragon_wear_4100\+_platform	1010
	snapdragon_x12_lte_modem	1011
	snapdragon_x24_lte_modem	1011
	snapdragon_x35_5g_modem-rf_system	1012

Vendor	Product	Page Number
Qualcomm	snapdragon_x50_5g_modem-rf_system	1013
	snapdragon_x55_5g_modem-rf_system	1014
	snapdragon_x62_5g_modem-rf_system	1016
	snapdragon_x65_5g_modem-rf_system	1017
	snapdragon_x70_modem-rf_system	1019
	snapdragon_x72_5g_modem-rf_system	1019
	snapdragon_x75_5g_modem-rf_system	1020
	snapdragon_xr1_platform	1022
	snapdragon_xr2\+_gen_1_platform	1023
	snapdragon_xr2_5g_platform	1024
	srv1h	1025
	srv1l	1027
	srv1m	1029
	ssg2115p	1031
	ssg2125p	1033
	sw5100	1034
	sw5100p	1036
	sxr1120	1037
	sxr1230p	1038
	sxr2130	1040
	sxr2230p	1041
	sxr2250p	1043
	talynplus	1044
	video_collaboration_vc1_platform	1046
	video_collaboration_vc3_platform	1047
	video_collaboration_vc5_platform	1049
	vision_intelligence_300_platform	1050
	vision_intelligence_400_platform	1051
	wcd9306	1053
	wcd9326	1053
	wcd9335	1055
	wcd9340	1056

Vendor	Product	Page Number
Qualcomm	csra6640_firmware	1775
	csrb31024_firmware	1776
	fastconnect_6200_firmware	1777
	fastconnect_6700_firmware	1778
	fastconnect_6800_firmware	1780
	fastconnect_6900_firmware	1781
	fastconnect_7800_firmware	1783
	flight_rb5_5g_platform_firmware	1785
	fsm10055_firmware	1787
	fsm10056_firmware	1787
	fsm20055_firmware	1788
	fsm20056_firmware	1788
	home_hub_100_platform_firmware	1788
	immersive_home_214_platform_firmware	1789
	immersive_home_216_platform_firmware	1790
	immersive_home_316_platform_firmware	1790
	immersive_home_318_platform_firmware	1791
	immersive_home_3210_platform_firmware	1792
	immersive_home_326_platform_firmware	1793
	ipq4018_firmware	1795
	ipq4019_firmware	1795
	ipq4028_firmware	1795
	ipq4029_firmware	1796
	ipq5010_firmware	1796
	ipq5028_firmware	1797
	ipq5300_firmware	1798
	ipq5302_firmware	1799
	ipq5312_firmware	1800
	ipq5332_firmware	1801
	ipq6000_firmware	1802
	ipq6005_firmware	1803
	ipq6010_firmware	1803

Vendor	Product	Page Number
Qualcomm	ipq6018_firmware	1804
	ipq6028_firmware	1806
	ipq8064_firmware	1807
	ipq8065_firmware	1807
	ipq8068_firmware	1807
	ipq8070a_firmware	1807
	ipq8070_firmware	1808
	ipq8071a_firmware	1809
	ipq8072a_firmware	1809
	ipq8074a_firmware	1810
	ipq8076a_firmware	1811
	ipq8076_firmware	1812
	ipq8078a_firmware	1813
	ipq8078_firmware	1814
	ipq8173_firmware	1815
	ipq8174_firmware	1816
	ipq9008_firmware	1817
	ipq9554_firmware	1818
	ipq9570_firmware	1819
	ipq9574_firmware	1820
	mdm9205s_firmware	1821
	mdm9628_firmware	1822
	mdm9640_firmware	1822
	mdm9650_firmware	1823
	msm8996au_firmware	1823
	pm8937_firmware	1824
	pmp8074_firmware	1824
	qam8255p_firmware	1824
	qam8295p_firmware	1827
	qam8620p_firmware	1828
	qam8650p_firmware	1830
	qam8775p_firmware	1832

Vendor	Product	Page Number
Qualcomm	qamsrv1h_firmware	1834
	qamsrv1m_firmware	1836
	qca0000_firmware	1838
	qca4004_firmware	1839
	qca4024_firmware	1840
	qca6174a_firmware	1841
	qca6234_firmware	1842
	qca6310_firmware	1843
	qca6320_firmware	1844
	qca6335_firmware	1845
	qca6391_firmware	1846
	qca6420_firmware	1848
	qca6421_firmware	1849
	qca6426_firmware	1850
	qca6430_firmware	1851
	qca6431_firmware	1852
	qca6436_firmware	1853
	qca6554a_firmware	1854
	qca6564au_firmware	1855
	qca6564a_firmware	1856
	qca6564_firmware	1858
	qca6574au_firmware	1858
	qca6574a_firmware	1860
	qca6574_firmware	1863
	qca6584au_firmware	1865
	qca6595au_firmware	1866
	qca6595_firmware	1868
	qca6678aq_firmware	1871
	qca6688aq_firmware	1873
	qca6696_firmware	1874
	qca6698aq_firmware	1876
	qca6797aq_firmware	1878

Vendor	Product	Page Number
Qualcomm	qca7500_firmware	1879
	qca8072_firmware	1880
	qca8075_firmware	1880
	qca8081_firmware	1881
	qca8082_firmware	1883
	qca8084_firmware	1885
	qca8085_firmware	1886
	qca8337_firmware	1887
	qca8386_firmware	1889
	qca9367_firmware	1890
	qca9377_firmware	1890
	qca9379_firmware	1891
	qca9880_firmware	1892
	qca9886_firmware	1892
	qca9888_firmware	1892
	qca9889_firmware	1893
	qca9898_firmware	1894
	qca9980_firmware	1894
	qca9984_firmware	1895
	qca9985_firmware	1895
	qca9990_firmware	1896
	qca9992_firmware	1896
	qca9994_firmware	1896
	qcc2073_firmware	1897
	qcc2076_firmware	1897
	qcc710_firmware	1898
	qcf8000_firmware	1899
	qcf8001_firmware	1900
	qcm2150_firmware	1901
	qcm2290_firmware	1902
	qcm4290_firmware	1903
	qcm4325_firmware	1905

Vendor	Product	Page Number
Qualcomm	qcm4490_firmware	1906
	qcm5430_firmware	1907
	qcm6125_firmware	1909
	qcm6490_firmware	1910
	qcm8550_firmware	1912
	qcn5021_firmware	1914
	qcn5022_firmware	1914
	qcn5024_firmware	1915
	qcn5052_firmware	1916
	qcn5054_firmware	1917
	qcn5121_firmware	1918
	qcn5122_firmware	1918
	qcn5124_firmware	1919
	qcn5152_firmware	1920
	qcn5154_firmware	1921
	qcn5164_firmware	1922
	qcn6023_firmware	1923
	qcn6024_firmware	1924
	qcn6100_firmware	1926
	qcn6102_firmware	1926
	qcn6112_firmware	1926
	qcn6122_firmware	1927
	qcn6132_firmware	1928
	qcn6224_firmware	1929
	qcn6274_firmware	1930
	qcn6402_firmware	1932
	qcn6412_firmware	1933
	qcn6422_firmware	1934
	qcn6432_firmware	1935
	qcn7606_firmware	1937
	qcn9000_firmware	1937
	qcn9001_firmware	1939

Vendor	Product	Page Number
Qualcomm	qcn9002_firmware	1939
	qcn9003_firmware	1939
	qcn9011_firmware	1940
	qcn9012_firmware	1941
	qcn9013_firmware	1942
	qcn9022_firmware	1942
	qcn9024_firmware	1943
	qcn9070_firmware	1945
	qcn9072_firmware	1946
	qcn9074_firmware	1947
	qcn9100_firmware	1949
	qcn9274_firmware	1949
	qcs2290_firmware	1951
	qcs410_firmware	1952
	qcs4290_firmware	1953
	qcs4490_firmware	1954
	qcs5430_firmware	1956
	qcs610_firmware	1957
	qcs6125_firmware	1958
	qcs6490_firmware	1960
	qcs7230_firmware	1961
	qcs8155_firmware	1963
	qcs8250_firmware	1964
	qcs8550_firmware	1965
	qdu1000_firmware	1967
	qdu1010_firmware	1968
	qdu1110_firmware	1969
	qdu1210_firmware	1970
	qdx1010_firmware	1971
	qdx1011_firmware	1972
	qep8111_firmware	1973
	qfw7114_firmware	1974

Vendor	Product	Page Number
Qualcomm	qfw7124_firmware	1975
	qrb5165m_firmware	1977
	qrb5165n_firmware	1978
	qru1032_firmware	1979
	qru1052_firmware	1980
	qru1062_firmware	1981
	qsm8250_firmware	1982
	qsm8350_firmware	1983
	qts110_firmware	1984
	qualcomm_205_mobile_platform_firmware	1985
	qualcomm_215_mobile_platform_firmware	1985
	robotics_rb3_platform_firmware	1985
	robotics_rb5_platform_firmware	1986
	sa4150p_firmware	1988
	sa4155p_firmware	1989
	sa6145p_firmware	1990
	sa6150p_firmware	1992
	sa6155p_firmware	1993
	sa6155_firmware	1994
	sa7255p_firmware	1995
	sa7775p_firmware	1998
	sa8145p_firmware	2000
	sa8150p_firmware	2001
	sa8155p_firmware	2002
	sa8155_firmware	2004
	sa8195p_firmware	2005
	sa8255p_firmware	2006
	sa8295p_firmware	2008
	sa8530p_firmware	2010
	sa8540p_firmware	2011
	sa8620p_firmware	2012
	sa8650p_firmware	2014

Vendor	Product	Page Number
Qualcomm	sa8770p_firmware	2016
	sa8775p_firmware	2018
	sa9000p_firmware	2020
	sc7180-ac_firmware	2022
	sc7180-ad_firmware	2023
	sc8180x-aa_firmware	2024
	sc8180x-ab_firmware	2024
	sc8180x-ac_firmware	2025
	sc8180x-ad_firmware	2026
	sc8180x-af_firmware	2027
	sc8180xp-aa_firmware	2028
	sc8180xp-ab_firmware	2028
	sc8180xp-ac_firmware	2029
	sc8180xp-ad_firmware	2030
	sc8180xp-af_firmware	2031
	sc8180x\+sdx55_firmware	2032
	sc8280xp-ab_firmware	2032
	sc8280xp-bb_firmware	2033
	sc8380xp_firmware	2034
	sd460_firmware	2034
	sd626_firmware	2035
	sd660_firmware	2035
	sd662_firmware	2036
	sd670_firmware	2037
	sd675_firmware	2038
	sd730_firmware	2039
	sd820_firmware	2040
	sd821_firmware	2040
	sd835_firmware	2040
	sd855_firmware	2041
	sd865_5g_firmware	2042
	sd888_firmware	2044

Vendor	Product	Page Number
Qualcomm	sdm429w_firmware	2045
	sdx55_firmware	2045
	sdx57m_firmware	2047
	sdx65m_firmware	2048
	sdx71m_firmware	2049
	sd_455_firmware	2049
	sd_675_firmware	2049
	sd_8cx_firmware	2050
	sd_8_gen1_5g_firmware	2051
	sg4150p_firmware	2052
	sg8275p_firmware	2054
	sm4125_firmware	2055
	sm4350-ac_firmware	2057
	sm6150-ac_firmware	2058
	sm6225-ad_firmware	2059
	sm6250p_firmware	2061
	sm6250_firmware	2062
	sm6370_firmware	2063
	sm7150-aa_firmware	2064
	sm7150-ab_firmware	2065
	sm7150-ac_firmware	2066
	sm7250-aa_firmware	2067
	sm7250-ab_firmware	2068
	sm7250-ac_firmware	2069
	sm7250p_firmware	2070
	sm7315_firmware	2072
	sm7325-ae_firmware	2073
	sm7325-af_firmware	2074
	sm7325p_firmware	2075
	sm8150-ac_firmware	2077
	sm8250-ab_firmware	2078
	sm8250-ac_firmware	2079

Vendor	Product	Page Number
Qualcomm	sm8350-ac_firmware	2080
	sm8550p_firmware	2082
	smart_audio_400_platform_firmware	2083
	snapdragon_210_processor_firmware	2085
	snapdragon_212_mobile_platform_firmware	2085
	snapdragon_425_mobile_platform_firmware	2086
	snapdragon_427_mobile_platform_firmware	2086
	snapdragon_429_mobile_platform_firmware	2086
	snapdragon_430_mobile_platform_firmware	2087
	snapdragon_435_mobile_platform_firmware	2087
	snapdragon_439_mobile_platform_firmware	2087
	snapdragon_450_mobile_platform_firmware	2088
	snapdragon_460_mobile_platform_firmware	2088
	snapdragon_480_5g_mobile_platform_firmware	2089
	snapdragon_4_gen_1_mobile_platform_firmware	2091
	snapdragon_4_gen_2_mobile_platform_firmware	2093
	snapdragon_625_mobile_platform_firmware	2094
	snapdragon_626_mobile_platform_firmware	2095
	snapdragon_630_mobile_platform_firmware	2095
	snapdragon_632_mobile_platform_firmware	2095
	snapdragon_636_mobile_platform_firmware	2095
	snapdragon_660_mobile_platform_firmware	2096
	snapdragon_662_mobile_platform_firmware	2096
	snapdragon_665_mobile_platform_firmware	2098
	snapdragon_670_mobile_platform_firmware	2099
	snapdragon_675_mobile_platform_firmware	2100
	snapdragon_680_4g_mobile_platform_firmware	2101
	snapdragon_690_5g_mobile_platform_firmware	2103

Vendor	Product	Page Number
Qualcomm	snapdragon_695_5g_mobile_platform_firmware	2104
	snapdragon_710_mobile_platform_firmware	2105
	snapdragon_712_mobile_platform_firmware	2106
	snapdragon_720g_mobile_platform_firmware	2107
	snapdragon_750g_5g_mobile_platform_firmware	2108
	snapdragon_778g_5g_mobile_platform_firmware	2109
	snapdragon_780g_5g_mobile_platform_firmware	2110
	snapdragon_7c\+_gen_3_compute_firmware	2111
	snapdragon_820_automotive_platform_firmware	2113
	snapdragon_820_mobile_platform_firmware	2113
	snapdragon_821_mobile_platform_firmware	2114
	snapdragon_835_mobile_pc_platform_firmware	2114
	snapdragon_845_mobile_platform_firmware	2115
	snapdragon_850_mobile_compute_platform_firmware	2116
	snapdragon_855_mobile_platform_firmware	2116
	snapdragon_865_5g_mobile_platform_firmware	2118
	snapdragon_888_5g_mobile_platform_firmware	2119
	snapdragon_8\+_gen_1_mobile_platform_firmware	2120
	snapdragon_8\+_gen_2_mobile_platform_firmware	2122
	snapdragon_8_gen_1_mobile_platform_firmware	2124
	snapdragon_8_gen_2_mobile_platform_firmware	2125
	snapdragon_8_gen_3_mobile_platform_firmware	2127

Vendor	Product	Page Number
Qualcomm	snapdragon_ar2_gen_1_platform_firmware	2129
	snapdragon_auto_4g_modem_firmware	2130
	snapdragon_auto_5g_modem-rf_firmware	2131
	snapdragon_auto_5g_modem-rf_gen_2_firmware	2132
	snapdragon_w5\+_gen_1_wearable_platform_firmware	2133
	snapdragon_wear_1300_platform_firmware	2134
	snapdragon_wear_4100\+_platform_firmware	2135
	snapdragon_x12_lte_modem_firmware	2136
	snapdragon_x24_lte_modem_firmware	2136
	snapdragon_x35_5g_modem-rf_system_firmware	2137
	snapdragon_x50_5g_modem-rf_system_firmware	2138
	snapdragon_x55_5g_modem-rf_system_firmware	2139
	snapdragon_x62_5g_modem-rf_system_firmware	2141
	snapdragon_x65_5g_modem-rf_system_firmware	2142
	snapdragon_x70_modem-rf_system_firmware	2144
	snapdragon_x72_5g_modem-rf_system_firmware	2144
	snapdragon_x75_5g_modem-rf_system_firmware	2145
	snapdragon_xr1_platform_firmware	2147
	snapdragon_xr2\+_gen_1_platform_firmware	2148
	snapdragon_xr2_5g_platform_firmware	2149
	srv1h_firmware	2150
	srv1l_firmware	2152
	srv1m_firmware	2154
	ssg2115p_firmware	2156
	ssg2125p_firmware	2158
	sw5100p_firmware	2159

Vendor	Product	Page Number
Qualcomm	sw5100_firmware	2161
	sxr1120_firmware	2162
	sxr1230p_firmware	2163
	sxr2130_firmware	2165
	sxr2230p_firmware	2166
	sxr2250p_firmware	2168
	talynplus_firmware	2169
	video_collaboration_vc1_platform_firmware	2171
	video_collaboration_vc3_platform_firmware	2172
	video_collaboration_vc5_platform_firmware	2174
	vision_intelligence_300_platform_firmware	2175
	vision_intelligence_400_platform_firmware	2176
	wcd9306_firmware	2178
	wcd9326_firmware	2178
	wcd9335_firmware	2180
	wcd9340_firmware	2181
	wcd9341_firmware	2183
	wcd9360_firmware	2184
	wcd9370_firmware	2185
	wcd9371_firmware	2186
	wcd9375_firmware	2187
	wcd9380_firmware	2188
	wcd9385_firmware	2190
	wcd9390_firmware	2192
	wcd9395_firmware	2194
	wcn3610_firmware	2196
	wcn3615_firmware	2196
	wcn3620_firmware	2197
	wcn3660b_firmware	2197
	wcn3660_firmware	2198
	wcn3680b_firmware	2198
	wcn3680_firmware	2199

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 10web					
Product: slider					
Affected Version(s): * Up to (excluding) 1.2.56					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2024	5.4	The Slider by 10Web WordPress plugin before 1.2.56 does not sanitise and escape some of its Slide options, which could allow authenticated users with access to the Sliders (by default Administrator, however this can be changed via the Slider by 10Web WordPress plugin before 1.2.56's options) and the ability to add images (Editor+) to perform Stored Cross-Site Scripting attacks **CVE ID: CVE-2024-6026**	N/A	A-10W-SLID-230724/1
Vendor: 2code					
Product: himer					
Affected Version(s): * Up to (excluding) 2.1.1					
Improper Neutralization of Input During Web Page Generation	03-Jul-2024	5.4	The Himer WordPress theme before 2.1.1 does not sanitise and escape some of its Post settings, which could allow high	N/A	A-2CO-HIME-230724/2

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
('Cross-site Scripting')			privilege users such as Contributor to perform Stored Cross-Site Scripting attacks **CVE ID: CVE-2024-2234**		
Cross-Site Request Forgery (CSRF)	03-Jul-2024	4.3	The Himer WordPress theme before 2.1.1 does not have CSRF checks in some places, which could allow attackers to make users join private groups via a CSRF attack **CVE ID: CVE-2024-2040**	N/A	A-2CO-HIME-230724/3
Cross-Site Request Forgery (CSRF)	03-Jul-2024	4.3	The Himer WordPress theme before 2.1.1 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks. These include declining and accepting group invitations or leaving a group **CVE ID: CVE-2024-2233**	N/A	A-2CO-HIME-230724/4
Cross-Site Request Forgery (CSRF)	03-Jul-2024	4.3	The Himer WordPress theme before 2.1.1 does not have CSRF checks in some	N/A	A-2CO-HIME-230724/5

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
			places, which could allow attackers to make users vote on any polls, including those they don't have access to via a CSRF attack **CVE ID: CVE-2024-2235**		
Product: wpqa_builder					
Affected Version(s): * Up to (excluding) 6.1.1					
Cross-Site Request Forgery (CSRF)	03-Jul-2024	8.8	The WPQA Builder WordPress plugin before 6.1.1 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks **CVE ID: CVE-2024-2376**	N/A	A-2CO-WPQA-230724/6
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jul-2024	5.4	The WPQA Builder WordPress plugin before 6.1.1 does not sanitise and escape some of its Slider settings, which could allow high privilege users such as contributor to perform Stored Cross-Site Scripting attacks **CVE ID: CVE-2024-2375**	N/A	A-2CO-WPQA-230724/7
Vendor: Apache					
Product: cloudstack					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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) 4.0.0 Up to (excluding) 4.18.2.1					
Improper Control of Generation of Code ('Code Injection')	05-Jul-2024	9.8	The CloudStack cluster service runs on unauthenticated port (default 9090) that can be misused to run arbitrary commands on targeted hypervisors and CloudStack management server hosts. Some of these commands were found to have command injection vulnerabilities that can result in arbitrary code execution via agents on the hosts that may run as a privileged user. An attacker that can reach the cluster service on the unauthenticated po rt (default 9090), can exploit this to perform remote code execution on CloudStack managed hosts and result in complete comprom ise of the confidentiality, integrity, and availability of CloudStack managed infrastructure.	N/A	A-APA-CLOU-230724/8

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Users are recommended to restrict the network access to the cluster service port (default 9090) on a CloudStack management server host to only its peer CloudStack management server hosts. Users are recommended to upgrade to version 4.18.2.1, 4.19.0.2 or later, which addresses this issue. **CVE ID: CVE-2024-38346**		
Improper Initialization	05-Jul-2024	9.8	The CloudStack integration API service allows running its unauthenticated API server (usually on port 8096 when configured and enabled via integration.api.port global setting) for internal portal integrations and for testing purposes. By default, the integration API service port is disabled and is considered disabled when integration.api.port	N/A	A-APA-CLOU-230724/9

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
			is set to 0 or negative. Due to an improper initialisation logic, the integration API service would listen on a random port when its port value is set to 0 (default value). An attacker that can access the CloudStack management network could scan and find the randomised integration API service port and exploit it to perform unauthorised administrative actions and perform remote code execution on CloudStack managed hosts and result in complete compromise of the confidentiality, integrity, and availability of CloudStack managed infrastructure. Users are recommended to restrict the network access on the CloudStack		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 server hosts to only essential ports. Users are recommended to upgrade to version 4.18.2.1, 4.19.0.2 or later, which addresses this issue. **CVE ID: CVE-2024-39864**		
Affected Version(s): From (including) 4.19.0.0 Up to (excluding) 4.19.0.2					
Improper Control of Generation of Code ('Code Injection')	05-Jul-2024	9.8	The CloudStack cluster service runs on unauthenticated port (default 9090) that can be misused to run arbitrary commands on targeted hypervisors and CloudStack management server hosts. Some of these commands were found to have command injection vulnerabilities that can result in arbitrary code execution via agents on the hosts that may run as a privileged user. An attacker that can reach the cluster service on the unauthenticated po rt (default 9090),	N/A	A-APA-CLOU-230724/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can exploit this to perform remote code execution on CloudStack managed hosts and result in complete compromise of the confidentiality, integrity, and availability of CloudStack managed infrastructure. Users are recommended to restrict the network access to the cluster service port (default 9090) on a CloudStack management server host to only its peer CloudStack management server hosts. Users are recommended to upgrade to version 4.18.2.1, 4.19.0.2 or later, which addresses this issue. **CVE ID: CVE-2024-38346**		
Improper Initialization	05-Jul-2024	9.8	The CloudStack integration API service allows running its unauthenticated	N/A	A-APA-CLOU-230724/11

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			API server (usually on port 8096 when configured and enabled via integration.api.port global setting) for internal portal integrations and for testing purposes. By default, the integration API service port is disabled and is considered disabled when integration.api.port is set to 0 or negative. Due to an improper initialisation logic, the integration API service would listen on a random port when its port value is set to 0 (default value). An attacker that can access the CloudStack management network could scan and find the randomised integration API service port and exploit it to perform unauthorised administrative actions and perform remote code execution on CloudStack managed hosts 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
			result in complete compromise of the confidentiality, integrity, and availability of CloudStack managed infrastructure. Users are recommended to restrict the network access on the CloudStack management server hosts to only essential ports. Users are recommended to upgrade to version 4.18.2.1, 4.19.0.2 or later, which addresses this issue. **CVE ID: CVE-2024-39864**		
Product: linkis					
Affected Version(s): From (including) 1.4.0 Up to (excluding) 1.6.0					
Deserialization of Untrusted Data	15-Jul-2024	8.8	In Apache Linkis <= 1.5.0, data source management module, when adding Mysql data source, exists remote code execution vulnerability for	https://lists.apache.org/thread/0dnzh64xy1n7qo3rgo2loz9zn7m9xgdx	A-APA-LINK-230724/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			java version < 1.8.0_241. The deserialization vulnerability exploited through jrmp can inject malicious files into the server and execute them. This attack requires the attacker to obtain an authorized account from Linkis before it can be carried out. We recommend that users upgrade the java version to >= 1.8.0_241. Or users upgrade Linkis to version 1.6.0. **CVE ID: CVE-2023-46801**		
Deserialization of Untrusted Data	15-Jul-2024	8.8	In Apache Linkis <=1.5.0, due to the lack of effective filtering of parameters, an attacker configuring malicious db2	https://lists.apache.org/thread/t68yy52lmv7pxgrxnq6rw7rwvk9tb1xj	A-APA-LINK-230724/13

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameters in the DataSource Manager Module will result in jndi injection. Therefore, the parameters in the DB2 URL should be blacklisted. This attack requires the attacker to obtain an authorized account from Linkis before it can be carried out. Versions of Apache Linkis <=1.5.0 will be affected. We recommend users upgrade the version of Linkis to version 1.6.0. **CVE ID: CVE-2023-49566**		
Files or Directories Accessible to External Parties	15-Jul-2024	6.5	In Apache Linkis =1.4.0, due to the lack of effective filtering of parameters, an attacker configuring	https://lists.apache.org/thread/dxkpwyoxy1jpdwlpqp15zvo0jxn4v729	A-APA-LINK-230724/14

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
			malicious Mysql JDBC parameters in the DataSource Manager Module will trigger arbitrary file reading. Therefore, the parameters in the Mysql JDBC URL should be blacklisted. This attack requires the attacker to obtain an authorized account from Linkis before it can be carried out. Versions of Apache Linkis = 1.4.0 will be affected. We recommend users upgrade the version of Linkis to version 1.5.0. **CVE ID: CVE-2023-41916**		
Product: nifi					
Affected Version(s): 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-2024	5.4	Apache NiFi 1.10.0 through 1.26.0 and 2.0.0-M1 through 2.0.0-M3 support a description field in the Parameter Context configuration that is vulnerable to cross-site scripting. An authenticated	N/A	A-APA-NIFI-230724/15

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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, authorized to configure a Parameter Context, can enter arbitrary JavaScript code, which the client browser will execute within the session context of the authenticated user. Upgrading to Apache NiFi 1.27.0 or 2.0.0-M4 is the recommended mitigation. **CVE ID: CVE-2024-37389**		
Affected Version(s): From (including) 1.10.0 Up to (excluding) 1.27.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-2024	5.4	Apache NiFi 1.10.0 through 1.26.0 and 2.0.0-M1 through 2.0.0-M3 support a description field in the Parameter Context configuration that is vulnerable to cross-site scripting. An authenticated user, authorized to configure a Parameter Context, can enter arbitrary JavaScript code, which the client browser will execute within the session context of the authenticated user. Upgrading to Apache NiFi 1.27.0 or 2.0.0-M4 is the	N/A	A-APA-NIFI-230724/16

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recommended mitigation. **CVE ID: CVE-2024-37389**		
Vendor: apollo13themes					
Product: rife_elementor_extensions_\&_templates					
Affected Version(s): * Up to (excluding) 1.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-2024	5.4	The Rife Elementor Extensions & Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tag' attribute within the plugin's Writing Effect Headline widget in all versions up to, and including, 1.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. 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-2024-5504**	https://plugins.trac.wordpress.org/changeset/3109903/#file1	A-APO-RIFE-230724/17
Vendor: axelerant					
Product: testimonials_widget					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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) 4.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Axelerant Testimonials Widget allows Stored XSS.This issue affects Testimonials Widget: from n/a through 4.0.4. **CVE ID: CVE-2024-37553**	N/A	A-AXE-TEST-230724/18
Vendor: ays-pro					
Product: secure_copy_content_protection_and_content_locking					
Affected Version(s): * Up to (excluding) 4.0.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2024	4.8	The Secure Copy Content Protection and Content Locking WordPress plugin before 4.0.9 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	N/A	A-AYS-SECU-230724/19

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
			CVE ID: CVE-2024-6138		
Vendor: b1ackc4t					
Product: 14finger					
Affected Version(s): 1.1					
N/A	05-Jul-2024	9.1	14Finger v1.1 was discovered to contain an arbitrary user deletion vulnerability via the component /api/admin/user?id. **CVE ID: CVE-2024-37768**	N/A	A-B1A-14FI-230724/20
N/A	05-Jul-2024	8.8	Insecure permissions in 14Finger v1.1 allow attackers to escalate privileges from normal user to Administrator via a crafted POST request. **CVE ID: CVE-2024-37769**	N/A	A-B1A-14FI-230724/21
Vendor: best_house_rental_management_system_project					
Product: best_house_rental_management_system					
Affected Version(s): * Up to (including) 1.0					
N/A	05-Jul-2024	7.5	Best House Rental Management System v1.0 was discovered to contain an arbitrary file read vulnerability via the Page parameter at index.php. This vulnerability	N/A	A-BES-BEST-230724/22

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows attackers to read arbitrary PHP files and access other sensitive information within the application. **CVE ID: CVE-2024-39210**		
Vendor: bible_text_project					
Product: bible_text					
Affected Version(s): * Up to (including) 0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2024	5.4	The Bible Text WordPress plugin through 0.2 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID: CVE-2024-5444**	N/A	A-BIB-BIBL-230724/23
Vendor: boot_store_project					
Product: boot_store					
Affected Version(s): * Up to (including) 1.6.4					
Improper Neutralization of Input During Web Page	02-Jul-2024	5.4	The Boot Store theme for WordPress is vulnerable to Stored Cross-Site	N/A	A-BOO-BOOT-230724/24

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')			Scripting via the 'link' parameter within the theme's Button shortcode in all versions up to, and including, 1.6.4 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-2024-5938**		
Vendor: cedcommerce					
Product: one_click_order_re-order					
Affected Version(s): * Up to (excluding) 1.1.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jul-2024	5.4	The One Click Order Re-Order plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ced_ocor_save_general_setting' function in all versions up to, and including, 1.1.9. This makes it	https://plugins.trac.wordpress.org/changeset/3110914/	A-CED-ONE_-230724/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible for authenticated attackers, with Subscriber-level access and above, to change the plugin settings, including adding stored cross-site scripting. **CVE ID: CVE-2024-5641**		
Vendor: cellopoint					
Product: secure_email_gateway					
Affected Version(s): * Up to (excluding) 4.5.0					
Out-of-bounds Write	15-Jul-2024	9.8	The SMTP Listener of Secure Email Gateway from Cellopoint does not properly validate user input, leading to a Buffer Overflow vulnerability. An unauthenticated remote attacker can exploit this vulnerability to execute arbitrary system commands on the remote server. **CVE ID: CVE-2024-6744**	N/A	A-CEL-SECU-230724/26
Vendor: codeastrology					
Product: ultraaddons					
Affected Version(s): * Up to (including) 1.1.6					
Improper Neutralization of Input	06-Jul-2024	5.4	Improper Neutralization of Input During Web	N/A	A-COD-ULTR-230724/27

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')			Page Generation (XSS or 'Cross-site Scripting') vulnerability in CodeAstrology Team UltraAddons Elementor Lite (Header & Footer Builder, Menu Builder, Cart Icon, Shortcode).This issue affects UltraAddons Elementor Lite (Header & Footer Builder, Menu Builder, Cart Icon, Shortcode): from n/a through 1.1.6. **CVE ID: CVE-2024-37554**		
Vendor: coderberg					
Product: residencecms					
Affected Version(s): 2.10.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-2024	5.4	A stored cross-site scripting (XSS) vulnerability exists in ResidenceCMS 2.10.1 that allows a low-privilege user to create malicious property content with HTML inside which acts as a stored XSS payload. **CVE ID: CVE-2024-39143**	https://github.com/Coderberg/ResidenceCMS/issues/128	A-COD-RESI-230724/28
Vendor: codermy					
Product: my-springsecurity-plus					
Affected Version(s): * Up to (excluding) 2024.07.03					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-Jul-2024	9.8	my-springsecurity-plus before v2024.07.03 was discovered to contain a SQL injection vulnerability via the dataScope parameter at /api/user. **CVE ID: CVE-2024-40539**	N/A	A-COD-MY-S-230724/29
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Jul-2024	9.8	my-springsecurity-plus before v2024.07.03 was discovered to contain a SQL injection vulnerability via the dataScope parameter at /api/dept. **CVE ID: CVE-2024-40540**	N/A	A-COD-MY-S-230724/30
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Jul-2024	9.8	my-springsecurity-plus before v2024.07.03 was discovered to contain a SQL injection vulnerability via the dataScope parameter at /api/dept/build. **CVE ID: CVE-2024-40541**	N/A	A-COD-MY-S-230724/31
Improper Neutralization of Special Elements used in an	12-Jul-2024	9.8	my-springsecurity-plus before v2024.07.03 was discovered to contain a SQL injection	N/A	A-COD-MY-S-230724/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			vulnerability via the dataScope parameter at /api/role?offset. **CVE ID: CVE-2024-40542**		
Vendor: davidlingren					
Product: media_library_assistant					
Affected Version(s): * Up to (excluding) 3.18					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-2024	6.1	The Media Library Assistant plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the order parameter in all versions up to, and including, 3.17 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-5544**	https://plugins.trac.wordpress.org/changeset/3110092/	A-DAV-MEDI-230724/33
Vendor: Dell					
Product: powerscale_onefs					
Affected Version(s): 9.8.0.0					

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
N/A	02-Jul-2024	6.7	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A local high privilege attacker could potentially exploit this vulnerability, leading to privilege escalation. **CVE ID: CVE-2024-32854**	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities	A-DEL-POWE-230724/34
N/A	02-Jul-2024	6.7	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A local high privileged attacker could potentially exploit this vulnerability, leading to unauthorized gain of root-level access. **CVE ID: CVE-2024-37126**	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities	A-DEL-POWE-230724/35
N/A	02-Jul-2024	6.7	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an incorrect privilege assignment vulnerability. A high privileged attacker with local access could potentially exploit	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-powerscale-onefs-for-multiple-	A-DEL-POWE-230724/36

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability, leading to Denial of service and Elevation of privileges. **CVE ID: CVE-2024-37132**	security-vulnerabilities	
N/A	02-Jul-2024	6.7	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A local high privileged attacker could potentially exploit this vulnerability, leading to unauthorized gain of root-level access. **CVE ID: CVE-2024-37133**	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities	A-DEL-POWE-230724/37
N/A	02-Jul-2024	6.7	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A local high privileged attacker could potentially exploit this vulnerability to gain root-level access. **CVE ID: CVE-2024-37134**	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities	A-DEL-POWE-230724/38
Affected Version(s): From (including) 8.2.0 Up to (excluding) 9.5.1.0					

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
Use of a Broken or Risky Cryptographic Algorithm	02-Jul-2024	7.5	Dell PowerScale OneFS versions 8.2.2.x through 9.7.0.0 contain use of a broken or risky cryptographic algorithm vulnerability. An unprivileged network malicious attacker could potentially exploit this vulnerability, leading to data leaks. **CVE ID: CVE-2024-32852**	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities	A-DEL-POWE-230724/39
Affected Version(s): From (including) 8.2.2 Up to (excluding) 9.4.0.18					
N/A	02-Jul-2024	7.8	Dell PowerScale OneFS versions 8.2.2.x through 9.7.0.2 contain an execution with unnecessary privileges vulnerability. A local low privileged attacker could potentially exploit this vulnerability, leading to escalation of privileges. **CVE ID: CVE-2024-32853**	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities	A-DEL-POWE-230724/40
N/A	02-Jul-2024	6.7	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-	A-DEL-POWE-230724/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local high privileged attacker could potentially exploit this vulnerability, leading to unauthorized gain of root-level access. **CVE ID: CVE-2024-37133**	powerscale-onefs-for-multiple-security-vulnerabilities	
Affected Version(s): From (including) 8.2.2 Up to (excluding) 9.5.1.0					
N/A	02-Jul-2024	6.7	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A local high privilege attacker could potentially exploit this vulnerability, leading to privilege escalation. **CVE ID: CVE-2024-32854**	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities	A-DEL-POWE-230724/42
N/A	02-Jul-2024	6.7	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an incorrect privilege assignment vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Denial of service and Elevation of privileges.	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities	A-DEL-POWE-230724/43

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-37132		
N/A	02-Jul-2024	6.7	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A local high privileged attacker could potentially exploit this vulnerability to gain root-level access. **CVE ID: CVE-2024-37134**	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities	A-DEL-POWE-230724/44
Affected Version(s): From (including) 8.2.2 Up to (excluding) 9.7.1.0					
N/A	02-Jul-2024	6.7	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A local high privileged attacker could potentially exploit this vulnerability, leading to unauthorized gain of root-level access. **CVE ID: CVE-2024-37126**	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities	A-DEL-POWE-230724/45
Affected Version(s): From (including) 9.5.0.0 Up to (excluding) 9.5.1.0					
N/A	02-Jul-2024	7.8	Dell PowerScale OneFS versions 8.2.2.x through 9.7.0.2 contain an execution with	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-	A-DEL-POWE-230724/46

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
			unnecessary privileges vulnerability. A local low privileged attacker could potentially exploit this vulnerability, leading to escalation of privileges. **CVE ID: CVE-2024-32853**	security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities	
N/A	02-Jul-2024	6.7	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A local high privileged attacker could potentially exploit this vulnerability, leading to unauthorized gain of root-level access. **CVE ID: CVE-2024-37133**	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities	A-DEL-POWE-230724/47
Affected Version(s): From (including) 9.6.0 Up to (excluding) 9.7.1.0					
N/A	02-Jul-2024	7.8	Dell PowerScale OneFS versions 8.2.2.x through 9.7.0.2 contain an execution with unnecessary privileges vulnerability. A local low privileged attacker could potentially exploit this vulnerability,	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities	A-DEL-POWE-230724/48

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
			leading to escalation of privileges. **CVE ID: CVE-2024-32853**		
Use of a Broken or Risky Cryptographic Algorithm	02-Jul-2024	7.5	Dell PowerScale OneFS versions 8.2.2.x through 9.7.0.0 contain use of a broken or risky cryptographic algorithm vulnerability. An unprivileged network malicious attacker could potentially exploit this vulnerability, leading to data leaks. **CVE ID: CVE-2024-32852**	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities	A-DEL-POWE-230724/49
N/A	02-Jul-2024	6.7	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A local high privilege attacker could potentially exploit this vulnerability, leading to privilege escalation. **CVE ID: CVE-2024-32854**	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities	A-DEL-POWE-230724/50
N/A	02-Jul-2024	6.7	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an incorrect privilege	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-	A-DEL-POWE-230724/51

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assignment vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Denial of service and Elevation of privileges. **CVE ID: CVE-2024-37132**	security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities	
N/A	02-Jul-2024	6.7	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A local high privileged attacker could potentially exploit this vulnerability, leading to unauthorized gain of root-level access. **CVE ID: CVE-2024-37133**	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities	A-DEL-POWE-230724/52
N/A	02-Jul-2024	6.7	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A local high privileged attacker could potentially exploit this vulnerability to	https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities	A-DEL-POWE-230724/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gain root-level access. **CVE ID: CVE-2024-37134**		
Vendor: delower					
Product: wp_to_do					
Affected Version(s): * Up to (including) 1.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Delower WP To Do allows Stored XSS.This issue affects WP To Do: from n/a through 1.3.0. **CVE ID: CVE-2024-37539**	N/A	A-DEL-WP_T-230724/54
Vendor: dj-extensions					
Product: dj-helpfularticles					
Affected Version(s): From (including) 1.0.0 Up to (including) 1.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	6.1	XSS vulnerability in DJ-HelpfulArticles component for Joomla. **CVE ID: CVE-2024-27183**	N/A	A-DJ--DJ-H-230724/55
Vendor: Docker					
Product: desktop					
Affected Version(s): * Up to (excluding) 4.29.0					
N/A	09-Jul-2024	7	In Docker Desktop before v4.29.0, an attacker who has	N/A	A-DOC-DESK-230724/56

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gained access to the Docker Desktop VM through a container breakout can further escape to the host by passing extensions and dashboard related IPC messages. Docker Desktop v4.29.0 https://docs.docker.com/desktop/release-notes/#4290 fixes the issue on MacOS, Linux and Windows with Hyper-V backend. As exploitation requires "Allow only extensions distributed through the Docker Marketplace" to be disabled, Docker Desktop v4.31.0 https://docs.docker.com/desktop/release-notes/#4310 additionally changes the default configuration to enable this setting by default. **CVE ID: CVE-2024-6222**		
Affected Version(s): * Up to (excluding) 4.31.0					

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	09-Jul-2024	5.5	In Docker Desktop on Windows before v4.31.0 allows a user in the docker-users group to cause a Windows Denial-of-Service through the exec-path Docker daemon config option in Windows containers mode. **CVE ID: CVE-2024-5652**	N/A	A-DOC-DESK-230724/57
Vendor: dotcamp					
Product: ultimate_blocks					
Affected Version(s): * Up to (excluding) 3.1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2024	5.4	The Ultimate Blocks WordPress plugin before 3.1.9 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID: CVE-2024-4655**	N/A	A-DOT-ULTI-230724/58
Affected Version(s): * Up to (excluding) 3.2.0					
Improper Neutralization of Input During	02-Jul-2024	5.4	The Ultimate Blocks – WordPress Blocks Plugin plugin for	N/A	A-DOT-ULTI-230724/59

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')			WordPress is vulnerable to Stored Cross-Site Scripting via the title tag parameter in all versions up to, and including, 3.1.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access and higher, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-3513**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-2024	5.4	The Ultimate Blocks – WordPress Blocks Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's blocks in all versions up to, and including, 3.1.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated	https://plugins.trac.wordpress.org/changeset/3075315/ultimate-blocks, https://plugins.trac.wordpress.org/changeset/3108401/	A-DOT-ULTI-230724/60

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2024-4268**		
Vendor: e4jconnect					
Product: vikrentcar					
Affected Version(s): * Up to (excluding) 1.3.2					
Cross-Site Request Forgery (CSRF)	11-Jul-2024	8.8	The VikRentCar Car Rental Management System WordPress plugin before 1.3.2 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks **CVE ID: CVE-2024-1845**	N/A	A-E4J-VIKR-230724/61
Vendor: ecommerce-codeigniter-bootstrap_project					
Product: ecommerce-codeigniter-bootstrap					
Affected Version(s): * Up to (excluding) 2024-07-03					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2024	6.1	A vulnerability classified as problematic has been found in CodeIgniter Ecommerce-CodeIgniter-Bootstrap up to	https://github.com/kirilkirkov/Ecommerce-CodeIgniter-Bootstrap/commit/1b3da45308bb6c3f55247d	A-ECO-ECOM-230724/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1998845073cf433bc6c250b0354461fbd84d0e03. This affects an unknown part. The manipulation of the argument search_title/catName/sub/name/categorie leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is 1b3da45308bb6c3f55247d0e99620b600bd85277. It is recommended to apply a patch to fix this issue. The identifier VDB-270369 was assigned to this vulnerability. **CVE ID: CVE-2024-6526**	0e99620b600bd85277	
Vendor: Egroupware					
Product: egroupware					
Affected Version(s): * Up to (excluding) 23.1.20240624					
N/A	07-Jul-2024	9.8	EGroupware before 23.1.20240624 mishandles an ORDER BY clause. This leads to json.php?menuaction=EGroupware\Api\Etemplate\Wid	https://github.com/EGroupware/egroupware/commit/553829d30cc2ccdc0e5a8c5a0e16fa03a3399a3f, https://github.c	A-EGR-EGRO-230724/63

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
			get\Nextmatch::ajax_get_rows sort.id SQL injection by authenticated users for Address Book or InfoLog sorting. **CVE ID: CVE-2024-40614**	om/EGroupware/egroupware/compare/23.1.20240430...23.1.20240624	
Vendor: elearningfreak					
Product: insert_or_embed_articulate_content					
Affected Version(s): * Up to (excluding) 4.3000000024					
Unrestricted Upload of File with Dangerous Type	15-Jul-2024	8.8	The Insert or Embed Articulate Content into WordPress plugin before 4.3000000024 does not prevent authors from uploading arbitrary files to the site, which may allow them to upload PHP shells on affected sites. **CVE ID: CVE-2024-5630**	N/A	A-ELE-INSE-230724/64
Vendor: electron					
Product: electron-builder					
Affected Version(s): * Up to (excluding) 6.3.0					
Improper Certificate Validation	09-Jul-2024	7.5	electron-updater allows for automatic updates for Electron apps. The file `packages/electron-updater/src/windowsExecutableCodeSignatureVerifier.ts	https://github.com/electron-userland/electron-builder/commit/ac2e6a25aa491c1ef5167a552c19fc2085cd427f, https://github.c	A-ELE-ELEC-230724/65

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
			` implements the signature validation routine for Electron applications on Windows. Because of the surrounding shell, a first pass by `cmd.exe` expands any environment variable found in command-line above. This creates a situation where `verifySignature()` can be tricked into validating the certificate of a different file than the one that was just downloaded. If the step is successful, the malicious update will be executed even if its signature is invalid. This attack assumes a compromised update manifest (server compromise, Man-in-the-Middle attack if fetched over HTTP, Cross-Site Scripting to point the application to a malicious updater server, etc.). The patch is available starting from 6.3.0-alpha.6.	om/electron-userland/electron-builder/pull/8295	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-39698		
Affected Version(s): 6.3.0					
Improper Certificate Validation	09-Jul-2024	7.5	electron-updater allows for automatic updates for Electron apps. The file `packages/electron-updater/src/windowsExecutableCodeSignatureVerifier.ts` implements the signature validation routine for Electron applications on Windows. Because of the surrounding shell, a first pass by `cmd.exe` expands any environment variable found in command-line above. This creates a situation where `verifySignature()` can be tricked into validating the certificate of a different file than the one that was just downloaded. If the step is successful, the malicious update will be executed even if its signature is invalid. This attack assumes a compromised update manifest	https://github.com/electron-userland/electron-builder/commit/ac2e6a25aa491c1ef5167a552c19fc2085cd427f, https://github.com/electron-userland/electron-builder/pull/8295	A-ELE-ELEC-230724/66

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 compromise, Man-in-the-Middle attack if fetched over HTTP, Cross-Site Scripting to point the application to a malicious updater server, etc.). The patch is available starting from 6.3.0-alpha.6. **CVE ID: CVE-2024-39698**		
Vendor: electronic_official_document_management_system_project					
Product: electronic_official_document_management_system					
Affected Version(s): * Up to (excluding) 5.0.77					
N/A	15-Jul-2024	8.8	The access control in the Electronic Official Document Management System from 2100 TECHNOLOGY is not properly implemented, allowing remote attackers with regular privileges to access the account settings functionality and create an administrator account. **CVE ID: CVE-2024-6737**	N/A	A-ELE-ELEC-230724/67
Vendor: embedded-solutions					
Product: freemodbus					
Affected Version(s): 2018-09-12					

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Jul-2024	7.5	Buffer Overflow vulnerability in SILA Embedded Solutions GmbH freemodbus v.2018-09-12 allows a remtoe attacker to cause a denial of service via the LINUXTCP server component. **CVE ID: CVE-2024-31504**	N/A	A-EMB-FREE-230724/68
Vendor: Exiv2					
Product: exiv2					
Affected Version(s): From (including) 0.28.0 Up to (excluding) 0.28.3					
Out-of-bounds Read	08-Jul-2024	6.5	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An out-of-bounds read was found in Exiv2 version v0.28.2. The vulnerability is in the parser for the ASF video format, which was a new feature in v0.28.0. The out-of-bounds read is triggered when Exiv2 is used to read the metadata of a crafted video file. The bug is fixed in version v0.28.3. **CVE ID: CVE-2024-39695**	https://github.com/Exiv2/exiv2/commit/3a28346db5ae1735a8728fe3491b0aecc1dbf387, https://github.com/Exiv2/exiv2/pull/3006, https://github.com/Exiv2/exiv2/security/advisories/GHSA-38rv-8x93-pvrh	A-EXI-EXIV-230724/69

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: expresstech					
Product: quiz_and_survey_master					
Affected Version(s): * Up to (excluding) 9.0.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jul-2024	8.8	The Quiz and Survey Master (QSM) WordPress plugin before 9.0.2 is vulnerable does not validate and escape the question_id parameter in the qsm_bulk_delete_question_from_database AJAX action, leading to a SQL injection exploitable by Contributors and above role **CVE ID: CVE-2024-5606**	N/A	A-EXP-QUIZ-230724/70
Affected Version(s): * Up to (excluding) 9.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2024	5.4	The Quiz and Survey Master (QSM) WordPress plugin before 9.0.5 does not sanitise and escape some of its Quiz settings, which could allow contributors and higher to perform Stored Cross-Site Scripting attacks **CVE ID: CVE-2024-6025**	N/A	A-EXP-QUIZ-230724/71
Vendor: flowiseai					
Product: flowise					
Affected Version(s): 1.4.3					

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 in Output Used by a Downstream Component ('Injection')	01-Jul-2024	7.5	Flowise is a drag & drop user interface to build a customized large language model flow. In version 1.4.3 of Flowise, the `/api/v1/openai-assistants-file` endpoint in `index.ts` is vulnerable to arbitrary file read due to lack of sanitization of the `fileName` body parameter. No known patches for this issue are available. **CVE ID: CVE-2024-36420**	N/A	A-FLO-FLOW-230724/72
Origin Validation Error	01-Jul-2024	7.5	Flowise is a drag & drop user interface to build a customized large language model flow. In version 1.4.3 of Flowise, A CORS misconfiguration sets the Access-Control-Allow-Origin header to all, allowing arbitrary origins to connect to the website. In the default configuration (unauthenticated), arbitrary origins may be able to make requests to	N/A	A-FLO-FLOW-230724/73

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Flowise, stealing information from the user. This CORS misconfiguration may be chained with the path injection to allow an attacker attackers without access to Flowise to read arbitrary files from the Flowise server. As of time of publication, no known patches are available. **CVE ID: CVE-2024-36421**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jul-2024	6.1	Flowise is a drag & drop user interface to build a customized large language model flow. In version 1.4.3 of Flowise, a reflected cross-site scripting vulnerability occurs in the `api/v1/chatflows/id` endpoint. If the default configuration is used (unauthenticated), an attacker may be able to craft a specially crafted URL that injects Javascript into the user sessions, allowing the attacker to steal	N/A	A-FLO-FLOW-230724/74

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
			information, create false popups, or even redirect the user to other websites without interaction. If the chatflow ID is not found, its value is reflected in the 404 page, which has type text/html. This allows an attacker to attach arbitrary scripts to the page, allowing an attacker to steal sensitive information. This XSS may be chained with the path injection to allow an attacker without direct access to Flowise to read arbitrary files from the Flowise server. As of time of publication, no known patches are available. **CVE ID: CVE-2024-36422**		
Vendor: gaizhenbiao					
Product: chuanhuchatgpt					
Affected Version(s): 20240410					
Improper Neutralization of Input During Web Page Generation	11-Jul-2024	6.1	A Stored Cross-Site Scripting (XSS) vulnerability exists in gaizhenbiao/chuanhuchatgpt version 20240410. This	N/A	A-GAI-CHUA-230724/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerability allows an attacker to inject malicious JavaScript code into the chat history file. When a victim uploads this file, the malicious script is executed in the victim's browser. This can lead to user data theft, session hijacking, malware distribution, and phishing attacks. **CVE ID: CVE-2024-6035**		
Vendor: Geoserver					
Product: geoserver					
Affected Version(s): * Up to (excluding) 2.23.6					
Improper Control of Generation of Code ('Code Injection')	01-Jul-2024	9.8	GeoServer is an open source server that allows users to share and edit geospatial data. Prior to versions 2.23.6, 2.24.4, and 2.25.2, multiple OGC request parameters allow Remote Code Execution (RCE) by unauthenticated users through specially crafted input against a default GeoServer installation due to unsafely evaluating property names as XPath expressions.	https://github.com/geoserver/geoserver/security/advisories/GHSA-6jj6-gm7p-fcvv, https://github.com/geotools/geotools/pull/4797, https://github.com/geotools/geotools/security/advisories/GHSA-w3pj-wh35-fq8w, https://osgeo-org.atlassian.net/browse/GEOT-7587	A-GEO-GEOS-230724/76

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 GeoTools library API that GeoServer calls evaluates property/attribute names for feature types in a way that unsafely passes them to the commons-jxpath library which can execute arbitrary code when evaluating XPath expressions. This XPath evaluation is intended to be used only by complex feature types (i.e., Application Schema data stores) but is incorrectly being applied to simple feature types as well which makes this vulnerability apply to **ALL** GeoServer instances. No public PoC is provided but this vulnerability has been confirmed to be exploitable through WFS GetFeature, WFS GetPropertyValue, WMS GetMap, WMS GetFeatureInfo, WMS GetLegendGraphic and WPS Execute requests. 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
			vulnerability can lead to executing arbitrary code. Versions 2.23.6, 2.24.4, and 2.25.2 contain a patch for the issue. A workaround exists by removing the `gt-complex-x.y.jar` file from the GeoServer where `x.y` is the GeoTools version (e.g., `gt-complex-31.1.jar` if running GeoServer 2.25.1). This will remove the vulnerable code from GeoServer but may break some GeoServer functionality or prevent GeoServer from deploying if the gt-complex module is needed. **CVE ID: CVE-2024-36401**		
Affected Version(s): From (including) 2.10.0 Up to (excluding) 2.24.4					
N/A	01-Jul-2024	4.9	GeoServer is an open source server that allows users to share and edit geospatial data. Starting in version 2.10.0 and prior to versions 2.24.4 and 2.25.1, GeoServer's Server Status page and REST API lists	https://github.com/geoserver/geoserver/security/advisories/GHSA-j59v-vgcr-hxvf	A-GEO-GEOS-230724/77

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 environment variables and Java properties to any GeoServer user with administrative rights as part of those modules' status message. These variables/properties can also contain sensitive information, such as database passwords or API keys/tokens. Additionally, many community-developed GeoServer container images `export` other credentials from their start-up scripts as environment variables to the GeoServer (`java`) process. The precise scope of the issue depends on which container image is used and how it is configured. The `about status` API endpoint which powers the Server Status page is only available to administrators.Depending on 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
			operating environment, administrators might have legitimate access to credentials in other ways, but this issue defeats more sophisticated controls (like break-glass access to secrets or role accounts).By default, GeoServer only allows same-origin authenticated API access. This limits the scope for a third-party attacker to use an administrator's credentials to gain access to credentials. The researchers who found the vulnerability were unable to determine any other conditions under which the GeoServer REST API may be available more broadly. Users should update container images to use GeoServer 2.24.4 or 2.25.1 to get the bug fix. As 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
			workaround, leave environment variables and Java system properties hidden by default. Those who provide the option to re-enable it should communicate the impact and risks so that users can make an informed choice. **CVE ID: CVE-2024-34696**		
Affected Version(s): From (including) 2.24.0 Up to (excluding) 2.24.4					
Improper Control of Generation of Code ('Code Injection')	01-Jul-2024	9.8	GeoServer is an open source server that allows users to share and edit geospatial data. Prior to versions 2.23.6, 2.24.4, and 2.25.2, multiple OGC request parameters allow Remote Code Execution (RCE) by unauthenticated users through specially crafted input against a default GeoServer installation due to unsafely evaluating property names as XPath expressions. The GeoTools library API that GeoServer calls evaluates property/attribute	https://github.com/geoserver/geoserver/security/advisories/GHSA-6jj6-gm7p-fcvv, https://github.com/geotools/geotools/pull/4797, https://github.com/geotools/geotools/security/advisories/GHSA-w3pj-wh35-fq8w, https://osgeo-org.atlassian.net/browse/GEOT-7587	A-GEO-GEOS-230724/78

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			names for feature types in a way that unsafely passes them to the commons-jxpath library which can execute arbitrary code when evaluating XPath expressions. This XPath evaluation is intended to be used only by complex feature types (i.e., Application Schema data stores) but is incorrectly being applied to simple feature types as well which makes this vulnerability apply to **ALL** GeoServer instances. No public PoC is provided but this vulnerability has been confirmed to be exploitable through WFS GetFeature, WFS GetPropertyValue, WMS GetMap, WMS GetFeatureInfo, WMS GetLegendGraphic and WPS Execute requests. This vulnerability can lead to executing arbitrary 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
			Versions 2.23.6, 2.24.4, and 2.25.2 contain a patch for the issue. A workaround exists by removing the `gt-complex-x.y.jar` file from the GeoServer where `x.y` is the GeoTools version (e.g., `gt-complex-31.1.jar` if running GeoServer 2.25.1). This will remove the vulnerable code from GeoServer but may break some GeoServer functionality or prevent GeoServer from deploying if the gt-complex module is needed. **CVE ID: CVE-2024-36401**		
Affected Version(s): From (including) 2.25.0 Up to (excluding) 2.25.1					
N/A	01-Jul-2024	4.9	GeoServer is an open source server that allows users to share and edit geospatial data. Starting in version 2.10.0 and prior to versions 2.24.4 and 2.25.1, GeoServer's Server Status page and REST API lists all environment variables and Java properties to any GeoServer user with administrative	https://github.com/geoserver/geoserver/security/advisories/GHSA-j59v-vgcr-hxvf	A-GEO-GEOS-230724/79

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
			rights as part of those modules' status message. These variables/properties can also contain sensitive information, such as database passwords or API keys/tokens. Additionally, many community-developed GeoServer container images `export` other credentials from their start-up scripts as environment variables to the GeoServer (`java`) process. The precise scope of the issue depends on which container image is used and how it is configured. The `about status` API endpoint which powers the Server Status page is only available to administrators.Depending on the operating environment, administrators might have legitimate access to		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 in other ways, but this issue defeats more sophisticated controls (like break-glass access to secrets or role accounts).By default, GeoServer only allows same-origin authenticated API access. This limits the scope for a third-party attacker to use an administrator's credentials to gain access to credentials. The researchers who found the vulnerability were unable to determine any other conditions under which the GeoServer REST API may be available more broadly. Users should update container images to use GeoServer 2.24.4 or 2.25.1 to get the bug fix. As a workaround, leave environment variables and Java system properties hidden by default.		

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Those who provide the option to re-enable it should communicate the impact and risks so that users can make an informed choice. **CVE ID: CVE-2024-34696**		
Affected Version(s): From (including) 2.25.0 Up to (excluding) 2.25.2					
Improper Control of Generation of Code ('Code Injection')	01-Jul-2024	9.8	GeoServer is an open source server that allows users to share and edit geospatial data. Prior to versions 2.23.6, 2.24.4, and 2.25.2, multiple OGC request parameters allow Remote Code Execution (RCE) by unauthenticated users through specially crafted input against a default GeoServer installation due to unsafely evaluating property names as XPath expressions. The GeoTools library API that GeoServer calls evaluates property/attribute names for feature types in a way that unsafely passes them to the commons-jxpath	https://github.com/geoserver/geoserver/security/advisories/GHSA-6jj6-gm7p-fcvv, https://github.com/geotools/geotools/pull/4797, https://github.com/geotools/geotools/security/advisories/GHSA-w3pj-wh35-fq8w, https://osgeo-org.atlassian.net/browse/GEOT-7587	A-GEO-GEOS-230724/80

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			library which can execute arbitrary code when evaluating XPath expressions. This XPath evaluation is intended to be used only by complex feature types (i.e., Application Schema data stores) but is incorrectly being applied to simple feature types as well which makes this vulnerability apply to **ALL** GeoServer instances. No public PoC is provided but this vulnerability has been confirmed to be exploitable through WFS GetFeature, WFS GetPropertyValue, WMS GetMap, WMS GetFeatureInfo, WMS GetLegendGraphic and WPS Execute requests. This vulnerability can lead to executing arbitrary code. Versions 2.23.6, 2.24.4, and 2.25.2 contain a patch for the issue. A workaround exists by removing 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
			`gt-complex-x.y.jar` file from the GeoServer where `x.y` is the GeoTools version (e.g., `gt-complex-31.1.jar` if running GeoServer 2.25.1). This will remove the vulnerable code from GeoServer but may break some GeoServer functionality or prevent GeoServer from deploying if the gt-complex module is needed. **CVE ID: CVE-2024-36401**		
Vendor: geotools					
Product: geotools					
Affected Version(s): * Up to (excluding) 29.6					
Improper Control of Generation of Code ('Code Injection')	01-Jul-2024	9.8	GeoServer is an open source server that allows users to share and edit geospatial data. Prior to versions 2.23.6, 2.24.4, and 2.25.2, multiple OGC request parameters allow Remote Code Execution (RCE) by unauthenticated users through specially crafted input against a default GeoServer installation due to unsafely evaluating	https://github.com/geoserver/geoserver/security/advisories/GHSA-6jj6-gm7p-fcvv, https://github.com/geotools/geotools/pull/4797, https://github.com/geotools/geotools/security/advisories/GHSA-w3pj-wh35-fq8w, https://osgeo-org.atlassian.net	A-GEO-GEOT-230724/81

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			property names as XPath expressions. The GeoTools library API that GeoServer calls evaluates property/attribute names for feature types in a way that unsafely passes them to the commons-jxpath library which can execute arbitrary code when evaluating XPath expressions. This XPath evaluation is intended to be used only by complex feature types (i.e., Application Schema data stores) but is incorrectly being applied to simple feature types as well which makes this vulnerability apply to **ALL** GeoServer instances. No public PoC is provided but this vulnerability has been confirmed to be exploitable through WFS GetFeature, WFS GetPropertyValue, WMS GetMap, WMS GetFeatureInfo, WMS	/browse/GEOT-7587	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GetLegendGraphic and WPS Execute requests. This vulnerability can lead to executing arbitrary code. Versions 2.23.6, 2.24.4, and 2.25.2 contain a patch for the issue. A workaround exists by removing the `gt-complex-x.y.jar` file from the GeoServer where `x.y` is the GeoTools version (e.g., `gt-complex-31.1.jar` if running GeoServer 2.25.1). This will remove the vulnerable code from GeoServer but may break some GeoServer functionality or prevent GeoServer from deploying if the gt-complex module is needed. **CVE ID: CVE-2024-36401**		
Affected Version(s): From (including) 30.0 Up to (excluding) 30.4					
Improper Control of Generation of Code ('Code Injection')	01-Jul-2024	9.8	GeoServer is an open source server that allows users to share and edit geospatial data. Prior to versions 2.23.6, 2.24.4, and 2.25.2, multiple	https://github.com/geoserver/geoserver/security/advisories/GHSA-6jj6-gm7p-fcvv, https://github.com/geotools/ge	A-GEO-GEOT-230724/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OGC request parameters allow Remote Code Execution (RCE) by unauthenticated users through specially crafted input against a default GeoServer installation due to unsafely evaluating property names as XPath expressions. The GeoTools library API that GeoServer calls evaluates property/attribute names for feature types in a way that unsafely passes them to the commons-jxpath library which can execute arbitrary code when evaluating XPath expressions. This XPath evaluation is intended to be used only by complex feature types (i.e., Application Schema data stores) but is incorrectly being applied to simple feature types as well which makes this vulnerability apply to **ALL** GeoServer instances. No	otools/pull/4797, https://github.com/geotools/geotools/security/advisories/GHSA-w3pj-wh35-fq8w, https://osgeo-org.atlassian.net/browse/GEOT-7587	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 PoC is provided but this vulnerability has been confirmed to be exploitable through WFS GetFeature, WFS GetPropertyValue, WMS GetMap, WMS GetFeatureInfo, WMS GetLegendGraphic and WPS Execute requests. This vulnerability can lead to executing arbitrary code. Versions 2.23.6, 2.24.4, and 2.25.2 contain a patch for the issue. A workaround exists by removing the `gt-complex-x.y.jar` file from the GeoServer where `x.y` is the GeoTools version (e.g., `gt-complex-31.1.jar` if running GeoServer 2.25.1). This will remove the vulnerable code from GeoServer but may break some GeoServer functionality or prevent GeoServer from deploying if the gt-complex module is needed.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-36401		
Affected Version(s): From (including) 31.0 Up to (excluding) 31.2					
Improper Control of Generation of Code ('Code Injection')	01-Jul-2024	9.8	GeoServer is an open source server that allows users to share and edit geospatial data. Prior to versions 2.23.6, 2.24.4, and 2.25.2, multiple OGC request parameters allow Remote Code Execution (RCE) by unauthenticated users through specially crafted input against a default GeoServer installation due to unsafely evaluating property names as XPath expressions. The GeoTools library API that GeoServer calls evaluates property/attribute names for feature types in a way that unsafely passes them to the commons-jxpath library which can execute arbitrary code when evaluating XPath expressions. This XPath evaluation is intended to be used only by complex	https://github.com/geoserver/geoserver/security/advisories/GHSA-6jj6-gm7p-fcvv, https://github.com/geotools/geotools/pull/4797, https://github.com/geotools/geotools/security/advisories/GHSA-w3pj-wh35-fq8w, https://osgeo-org.atlassian.net/browse/GEOT-7587	A-GEO-GEOT-230724/83

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
			feature types (i.e., Application Schema data stores) but is incorrectly being applied to simple feature types as well which makes this vulnerability apply to **ALL** GeoServer instances. No public PoC is provided but this vulnerability has been confirmed to be exploitable through WFS GetFeature, WFS GetPropertyValue, WMS GetMap, WMS GetFeatureInfo, WMS GetLegendGraphic and WPS Execute requests. This vulnerability can lead to executing arbitrary code. Versions 2.23.6, 2.24.4, and 2.25.2 contain a patch for the issue. A workaround exists by removing the `gt-complex-x.y.jar` file from the GeoServer where `x.y` is the GeoTools version (e.g., `gt-complex-31.1.jar` if running GeoServer 2.25.1). This will		

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remove the vulnerable code from GeoServer but may break some GeoServer functionality or prevent GeoServer from deploying if the gt-complex module is needed. **CVE ID: CVE-2024-36401**		
Vendor: Gitlab					
Product: gitlab					
Affected Version(s): From (including) 15.8.0 Up to (excluding) 16.11.6					
N/A	11-Jul-2024	9.8	An issue was discovered in GitLab CE/EE affecting all versions starting from 15.8 prior to 16.11.6, starting from 17.0 prior to 17.0.4, and starting from 17.1 prior to 17.1.2, which allows an attacker to trigger a pipeline as another user under certain circumstances. **CVE ID: CVE-2024-6385**	N/A	A-GIT-GITL-230724/84
Affected Version(s): From (including) 16.5.0 Up to (excluding) 16.11.6					
N/A	11-Jul-2024	2.7	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.5 prior to 16.11.6, starting	N/A	A-GIT-GITL-230724/85

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from 17.0 prior to 17.0.4, and starting from 17.1 prior to 17.1.2 in which a user with `admin_group_member` custom role permission could ban group members. **CVE ID: CVE-2024-2880**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.4					
N/A	11-Jul-2024	9.8	An issue was discovered in GitLab CE/EE affecting all versions starting from 15.8 prior to 16.11.6, starting from 17.0 prior to 17.0.4, and starting from 17.1 prior to 17.1.2, which allows an attacker to trigger a pipeline as another user under certain circumstances. **CVE ID: CVE-2024-6385**	N/A	A-GIT-GITL-230724/86
N/A	11-Jul-2024	2.7	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.5 prior to 16.11.6, starting from 17.0 prior to 17.0.4, and starting from 17.1 prior to 17.1.2 in which a	N/A	A-GIT-GITL-230724/87

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user with `admin_group_member` custom role permission could ban group members. **CVE ID: CVE-2024-2880**		
N/A	11-Jul-2024	2.7	An issue was discovered in GitLab CE/EE affecting all versions starting from 17.0 prior to 17.0.4 and from 17.1 prior to 17.1.2 where a Developer user with `admin_compliance_framework` custom role may have been able to modify the URL for a group namespace. **CVE ID: CVE-2024-5257**	N/A	A-GIT-GITL-230724/88
N/A	11-Jul-2024	2.7	An issue was discovered in GitLab CE/EE affecting all versions starting from 17.0 prior to 17.0.4 and from 17.1 prior to 17.1.2 where a Guest user with `admin_push_rules` permission may have been able to create project-level deploy tokens.	N/A	A-GIT-GITL-230724/89

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
			CVE ID: CVE-2024-5470		
Affected Version(s): From (including) 17.1.0 Up to (excluding) 17.1.2					
N/A	11-Jul-2024	9.8	An issue was discovered in GitLab CE/EE affecting all versions starting from 15.8 prior to 16.11.6, starting from 17.0 prior to 17.0.4, and starting from 17.1 prior to 17.1.2, which allows an attacker to trigger a pipeline as another user under certain circumstances. **CVE ID: CVE-2024-6385**	N/A	A-GIT-GITL-230724/90
N/A	11-Jul-2024	2.7	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.5 prior to 16.11.6, starting from 17.0 prior to 17.0.4, and starting from 17.1 prior to 17.1.2 in which a user with `admin_group_member` custom role permission could ban group members. **CVE ID: CVE-2024-2880**	N/A	A-GIT-GITL-230724/91
N/A	11-Jul-2024	2.7	An issue was discovered in	N/A	A-GIT-GITL-230724/92

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 CE/EE affecting all versions starting from 17.0 prior to 17.0.4 and from 17.1 prior to 17.1.2 where a Developer user with `admin_compliance_framework` custom role may have been able to modify the URL for a group namespace. **CVE ID: CVE-2024-5257**		
N/A	11-Jul-2024	2.7	An issue was discovered in GitLab CE/EE affecting all versions starting from 17.0 prior to 17.0.4 and from 17.1 prior to 17.1.2 where a Guest user with `admin_push_rules` permission may have been able to create project-level deploy tokens. **CVE ID: CVE-2024-5470**	N/A	A-GIT-GITL-230724/93
Vendor: goanother					
Product: another_redis_desktop_manager					
Affected Version(s): * Up to (including) 1.6.1					
Improper Neutralization of Input During Web Page Generation	05-Jul-2024	9.6	goanother Another Redis Desktop Manager =<1.6.1 is vulnerable to Cross Site Scripting (XSS) via	N/A	A-GOA-ANOT-230724/94

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
('Cross-site Scripting')			src/components/Setting.vue. **CVE ID: CVE-2024-23998**		
Vendor: hcltech					
Product: domino					
Affected Version(s): 11.0					
N/A	08-Jul-2024	7.5	This vulnerability is being re-assessed. Vulnerability details will be updated. The security bulletin will be republished when further details are available. **CVE ID: CVE-2024-23562**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0113822	A-HCL-DOMI-230724/95
Affected Version(s): 12.0					
N/A	08-Jul-2024	7.5	This vulnerability is being re-assessed. Vulnerability details will be updated. The security bulletin will be republished when further details are available. **CVE ID: CVE-2024-23562**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0113822	A-HCL-DOMI-230724/96
Affected Version(s): 14.0					
N/A	08-Jul-2024	7.5	This vulnerability is being re-assessed. Vulnerability details will be updated.	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0113822	A-HCL-DOMI-230724/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The security bulletin will be republished when further details are available. **CVE ID: CVE-2024-23562**		
Product: nomad_server_on_domino					
Affected Version(s): * Up to (excluding) 1.0.12					
N/A	05-Jul-2024	6.5	HCL Nomad server on Domino fails to properly handle users configured with limited Domino access resulting in a possible denial of service vulnerability. **CVE ID: CVE-2024-23588**	N/A	A-HCL-NOMA-230724/98
Vendor: heyewei					
Product: springbootcms					
Affected Version(s): * Up to (including) 2024-05-28					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2024	4.8	A vulnerability classified as problematic has been found in heyewei SpringBootCMS up to 2024-05-28. Affected is an unknown function of the file /guestbook of the component Guestbook Handler. The manipulation of the argument Content leads to cross site scripting.	N/A	A-HEY-SPRI-230724/99

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-270450 is the identifier assigned to this vulnerability. **CVE ID: CVE-2024-6539**		
Vendor: hitout					
Product: carsale					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jul-2024	6.5	A vulnerability has been found in Hitout Carsale 1.0 and classified as critical. This vulnerability affects unknown code of the file OrderController.java. The manipulation of the argument orderBy leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-270166 is the identifier assigned to this vulnerability. **CVE ID: CVE-2024-6438**	N/A	A-HIT-CARS-230724/100
Vendor: home_owners_collection_management_system_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: home_owners_collection_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	02-Jul-2024	9.8	A vulnerability was found in SourceCodester Home Owners Collection Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /classes/Users.php?f=save. The manipulation of the argument img leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-270167. **CVE ID: CVE-2024-6439**	N/A	A-HOM-HOME-230724/101
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jul-2024	9.8	A vulnerability was found in SourceCodester Home Owners Collection Management System 1.0. It has been classified as critical. Affected is an unknown function of the file	N/A	A-HOM-HOME-230724/102

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/classes/Master.php?f=delete_category. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-270168. **CVE ID: CVE-2024-6440**		
Vendor: IBM					
Product: cloud_pak_for_business_automation					
Affected Version(s): 21.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-2024	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading	https://exchange.xforce.ibmcloud.com/vulnerabilities/294293, https://www.ibm.com/support/pages/node/7159332	A-IBM-CLOU-230724/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to credentials disclosure within a trusted session. IBM X-Force ID: 294293. **CVE ID: CVE-2024-37528**		
Server-Side Request Forgery (SSRF)	08-Jul-2024	4.3	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 288178. **CVE ID: CVE-2024-31897**	https://exchange.xforce.ibmcloud.com/vulnerabilities/288178, https://www.ibm.com/support/pages/node/7159332	A-IBM-CLOU-230724/104
Affected Version(s): 21.0.3					
Improper Neutralization of Input During Web Page Generation	08-Jul-2024	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3,	https://exchange.xforce.ibmcloud.com/vulnerabilities/294293, https://www.ibm.com/support	A-IBM-CLOU-230724/105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 294293. **CVE ID: CVE-2024-37528**	/pages/node/7159332	
Server-Side Request Forgery (SSRF)	08-Jul-2024	4.3	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network	https://exchange.xforce.ibmcloud.com/vulnerabilities/288178, https://www.ibm.com/support/pages/node/7159332	A-IBM-CLOU-230724/106

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enumeration or facilitating other attacks. IBM X-Force ID: 288178. **CVE ID: CVE-2024-31897**		
Affected Version(s): 22.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-2024	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 294293. **CVE ID: CVE-2024-37528**	https://exchange.xforce.ibmcloud.com/vulnerabilities/294293, https://www.ibm.com/support/pages/node/7159332	A-IBM-CLOU-230724/107
Server-Side Request Forgery (SSRF)	08-Jul-2024	4.3	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1,	https://exchange.xforce.ibmcloud.com/vulnerabilities/288178, https://www.ibm.com/support	A-IBM-CLOU-230724/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 288178. **CVE ID: CVE-2024-31897**	/pages/node/7159332	
Affected Version(s): 22.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-2024	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality	https://exchange.xforce.ibmcloud.com/vulnerabilities/294293, https://www.ibm.com/support/pages/node/7159332	A-IBM-CLOU-230724/109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 294293. **CVE ID: CVE-2024-37528**		
Server-Side Request Forgery (SSRF)	08-Jul-2024	4.3	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 288178. **CVE ID: CVE-2024-31897**	https://exchange.xforce.ibmcloud.com/vulnerabilities/288178, https://www.ibm.com/support/pages/node/7159332	A-IBM-CLOU-230724/110
Affected Version(s): 23.0.1					
Improper Neutralization of Input During Web Page Generation	08-Jul-2024	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1,	https://exchange.xforce.ibmcloud.com/vulnerabilities/294293, https://www.ibm.com/support	A-IBM-CLOU-230724/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 294293. **CVE ID: CVE-2024-37528**	/pages/node/7159332	
Server-Side Request Forgery (SSRF)	08-Jul-2024	4.3	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially	https://exchange.xforce.ibmcloud.com/vulnerabilities/288178, https://www.ibm.com/support/pages/node/7159332	A-IBM-CLOU-230724/112

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
			leading to network enumeration or facilitating other attacks. IBM X-Force ID: 288178. **CVE ID: CVE-2024-31897**		
Affected Version(s): 23.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-2024	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 294293. **CVE ID: CVE-2024-37528**	https://exchange.xforce.ibmcloud.com/vulnerabilities/294293, https://www.ibm.com/support/pages/node/7159332	A-IBM-CLOU-230724/113
Server-Side Request Forgery (SSRF)	08-Jul-2024	4.3	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2,	https://exchange.xforce.ibmcloud.com/vulnerabilities/288178, https://www.ib	A-IBM-CLOU-230724/114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 288178. **CVE ID: CVE-2024-31897**	m.com/support/pages/node/7159332	
Affected Version(s): From (including) 18.0.0 Up to (including) 18.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-2024	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended	https://exchange.xforce.ibmcloud.com/vulnerabilities/294293, https://www.ibm.com/support/pages/node/7159332	A-IBM-CLOU-230724/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 294293. **CVE ID: CVE-2024-37528**		
Server-Side Request Forgery (SSRF)	08-Jul-2024	4.3	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 288178. **CVE ID: CVE-2024-31897**	https://exchange.xforce.ibmcloud.com/vulnerabilities/288178, https://www.ibm.com/support/pages/node/7159332	A-IBM-CLOU-230724/116
Affected Version(s): From (including) 19.0.1 Up to (including) 19.0.3					
Improper Neutralization of Input During Web Page	08-Jul-2024	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2,	https://exchange.xforce.ibmcloud.com/vulnerabilities/294293, https://www.ib	A-IBM-CLOU-230724/117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 294293. **CVE ID: CVE-2024-37528**	m.com/support/pages/node/7159332	
Server-Side Request Forgery (SSRF)	08-Jul-2024	4.3	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the	https://exchange.xforce.ibmcloud.com/vulnerabilities/288178, https://www.ibm.com/support/pages/node/7159332	A-IBM-CLOU-230724/118

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 288178. **CVE ID: CVE-2024-31897**		
Affected Version(s): From (including) 20.0.1 Up to (including) 20.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-2024	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 294293. **CVE ID: CVE-2024-37528**	https://exchange.xforce.ibmcloud.com/vulnerabilities/294293, https://www.ibm.com/support/pages/node/7159332	A-IBM-CLOU-230724/119
Server-Side Request	08-Jul-2024	4.3	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2,	https://exchange.xforce.ibmcloud.com/vulnerabilities/288178,	A-IBM-CLOU-230724/120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 288178. **CVE ID: CVE-2024-31897**	https://www.ibm.com/support/pages/node/7159332	
Product: datacap					
Affected Version(s): 9.1.5					
Improper Encoding or Escaping of Output	15-Jul-2024	9.8	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or	https://exchange.xforce.ibmcloud.com/vulnerabilities/296003, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/121

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session hijacking. IBM X-Force ID: 296003. **CVE ID: CVE-2024-39736**		
Use of a Broken or Risky Cryptographic Algorithm	15-Jul-2024	7.5	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 295970. **CVE ID: CVE-2024-39731**	https://exchange.xforce.ibmcloud.com/vulnerabilities/295970	A-IBM-DATA-230724/122
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Jul-2024	5.4	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 295967.	https://exchange.xforce.ibmcloud.com/vulnerabilities/295967, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/123

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-39728		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Jul-2024	5.4	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 296002. **CVE ID: CVE-2024-39735**	https://exchange.xforce.ibmcloud.com/vulnerabilities/296002, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/124
Generation of Error Message Containing Sensitive Information	15-Jul-2024	5.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 296004.	https://exchange.xforce.ibmcloud.com/vulnerabilities/296004, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39737		
N/A	15-Jul-2024	5.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 displays version information in HTTP requests that could allow an attacker to gather information for future attacks against the system. IBM X-Force ID: 296009. **CVE ID: CVE-2024-39740**	https://exchange.xforce.ibmcloud.com/vulnerabilities/296009, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/126
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	15-Jul-2024	5.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 could allow a remote attacker 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. IBM X-Force ID: 296010. **CVE ID: CVE-2024-39741**	https://exchange.xforce.ibmcloud.com/vulnerabilities/296010, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/127
Server-Side Request Forgery (SSRF)	15-Jul-2024	4.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to	https://exchange.xforce.ibmcloud.com/vulnerabilities/296008, https://www.ib	A-IBM-DATA-230724/128

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
			server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 296008. **CVE ID: CVE-2024-39739**	m.com/support/pages/node/7160185	
N/A	15-Jul-2024	4.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 could allow an authenticated user to obtain sensitive information from source code that could be used in further attacks against the system. IBM X-Force ID: 295968. **CVE ID: CVE-2024-39729**	https://exchange.xforce.ibmcloud.com/vulnerabilities/295968, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/129
Affected Version(s): 9.1.6					
Improper Encoding or Escaping of Output	15-Jul-2024	9.8	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST	https://exchange.xforce.ibmcloud.com/vulnerabilities/296003, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/130

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
			headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 296003. **CVE ID: CVE-2024-39736**		
Use of a Broken or Risky Cryptographic Algorithm	15-Jul-2024	7.5	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 295970. **CVE ID: CVE-2024-39731**	https://exchange.xforce.ibmcloud.com/vulnerabilities/295970	A-IBM-DATA-230724/131
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Jul-2024	5.4	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended	https://exchange.xforce.ibmcloud.com/vulnerabilities/295967, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/132

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
			functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 295967. **CVE ID: CVE-2024-39728**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Jul-2024	5.4	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 296002. **CVE ID: CVE-2024-39735**	https://exchange.xforce.ibmcloud.com/vulnerabilities/296002, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/133
Generation of Error Message Containing Sensitive Information	15-Jul-2024	5.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the	https://exchange.xforce.ibmcloud.com/vulnerabilities/296004, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			browser. This information could be used in further attacks against the system. IBM X-Force ID: 296004. **CVE ID: CVE-2024-39737**		
N/A	15-Jul-2024	5.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 displays version information in HTTP requests that could allow an attacker to gather information for future attacks against the system. IBM X-Force ID: 296009. **CVE ID: CVE-2024-39740**	https://exchange.xforce.ibmcloud.com/vulnerabilities/296009, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/135
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	15-Jul-2024	5.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 could allow a remote attacker 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. IBM X-Force ID: 296010.	https://exchange.xforce.ibmcloud.com/vulnerabilities/296010, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/136

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-39741		
Server-Side Request Forgery (SSRF)	15-Jul-2024	4.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 296008. **CVE ID: CVE-2024-39739**	https://exchange.xforce.ibmcloud.com/vulnerabilities/296008, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/137
N/A	15-Jul-2024	4.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 could allow an authenticated user to obtain sensitive information from source code that could be used in further attacks against the system. IBM X-Force ID: 295968. **CVE ID: CVE-2024-39729**	https://exchange.xforce.ibmcloud.com/vulnerabilities/295968, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/138
Affected Version(s): 9.1.7					
Improper Encoding or	15-Jul-2024	9.8	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8,	https://exchange.xforce.ibmcloud.com/vulnerab	A-IBM-DATA-230724/139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Escaping of Output			and 9.1.9 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 296003. **CVE ID: CVE-2024-39736**	ilities/296003, https://www.ibm.com/support/pages/node/7160185	
Use of a Broken or Risky Cryptographic Algorithm	15-Jul-2024	7.5	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 295970. **CVE ID: CVE-2024-39731**	https://exchange.xforce.ibmcloud.com/vulnerabilities/295970	A-IBM-DATA-230724/140
Improper Neutralization of Input During Web Page Generation	15-Jul-2024	5.4	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to stored cross-site scripting. This	https://exchange.xforce.ibmcloud.com/vulnerabilities/295967, https://www.ibm.com/support	A-IBM-DATA-230724/141

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
('Cross-site Scripting')			vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 295967. **CVE ID: CVE-2024-39728**	/pages/node/7160185	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Jul-2024	5.4	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 296002. **CVE ID: CVE-2024-39735**	https://exchange.xforce.ibmcloud.com/vulnerabilities/296002, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/142
Generation of Error Message Containing	15-Jul-2024	5.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 could	https://exchange.xforce.ibmcloud.com/vulnerabilities/296004,	A-IBM-DATA-230724/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 296004. **CVE ID: CVE-2024-39737**	https://www.ibm.com/support/pages/node/7160185	
N/A	15-Jul-2024	5.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 displays version information in HTTP requests that could allow an attacker to gather information for future attacks against the system. IBM X-Force ID: 296009. **CVE ID: CVE-2024-39740**	https://exchange.xforce.ibmcloud.com/vulnerabilities/296009, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/144
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	15-Jul-2024	5.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot	https://exchange.xforce.ibmcloud.com/vulnerabilities/296010, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 296010. **CVE ID: CVE-2024-39741**		
Server-Side Request Forgery (SSRF)	15-Jul-2024	4.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 296008. **CVE ID: CVE-2024-39739**	https://exchange.xforce.ibmcloud.com/vulnerabilities/296008, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/146
N/A	15-Jul-2024	4.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 could allow an authenticated user to obtain sensitive information from source code that could be used in further attacks against the system. IBM X-Force ID: 295968.	https://exchange.xforce.ibmcloud.com/vulnerabilities/295968, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39729		
Affected Version(s): 9.1.8					
Improper Encoding or Escaping of Output	15-Jul-2024	9.8	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 296003. **CVE ID: CVE-2024-39736**	https://exchange.xforce.ibmcloud.com/vulnerabilities/296003, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/148
Use of a Broken or Risky Cryptographic Algorithm	15-Jul-2024	7.5	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 295970. **CVE ID: CVE-2024-39731**	https://exchange.xforce.ibmcloud.com/vulnerabilities/295970	A-IBM-DATA-230724/149

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	15-Jul-2024	5.4	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 295967. **CVE ID: CVE-2024-39728**	https://exchange.xforce.ibmcloud.com/vulnerabilities/295967, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/150
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Jul-2024	5.4	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	https://exchange.xforce.ibmcloud.com/vulnerabilities/296002, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 296002. **CVE ID: CVE-2024-39735**		
Generation of Error Message Containing Sensitive Information	15-Jul-2024	5.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 296004. **CVE ID: CVE-2024-39737**	https://exchange.xforce.ibmcloud.com/vulnerabilities/296004, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/152
N/A	15-Jul-2024	5.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 displays version information in HTTP requests that could allow an attacker to gather information for future attacks against the system. IBM X-Force ID: 296009. **CVE ID: CVE-2024-39740**	https://exchange.xforce.ibmcloud.com/vulnerabilities/296009, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/153
Improper Limitation of a	15-Jul-2024	5.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8,	https://exchange.xforce.ibmcloud.com/vulnerab	A-IBM-DATA-230724/154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			and 9.1.9 could allow a remote attacker 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. IBM X-Force ID: 296010. **CVE ID: CVE-2024-39741**	ilities/296010, https://www.ibm.com/support/pages/node/7160185	
Server-Side Request Forgery (SSRF)	15-Jul-2024	4.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 296008. **CVE ID: CVE-2024-39739**	https://exchange.xforce.ibmcloud.com/vulnerabilities/296008, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/155
N/A	15-Jul-2024	4.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 could allow an authenticated user to obtain sensitive	https://exchange.xforce.ibmcloud.com/vulnerabilities/295968, https://www.ibm.com/support	A-IBM-DATA-230724/156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information from source code that could be used in further attacks against the system. IBM X-Force ID: 295968. **CVE ID: CVE-2024-39729**	/pages/node/7160185	
Affected Version(s): 9.1.9					
Improper Encoding or Escaping of Output	15-Jul-2024	9.8	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 296003. **CVE ID: CVE-2024-39736**	https://exchange.xforce.ibmcloud.com/vulnerabilities/296003, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/157
Use of a Broken or Risky Cryptographic Algorithm	15-Jul-2024	7.5	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 uses weaker than expected cryptographic algorithms that could allow an	https://exchange.xforce.ibmcloud.com/vulnerabilities/295970	A-IBM-DATA-230724/158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to decrypt highly sensitive information. IBM X-Force ID: 295970. **CVE ID: CVE-2024-39731**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Jul-2024	5.4	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 295967. **CVE ID: CVE-2024-39728**	https://exchange.xforce.ibmcloud.com/vulnerabilities/295967, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/159
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Jul-2024	5.4	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the	https://exchange.xforce.ibmcloud.com/vulnerabilities/296002, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 296002. **CVE ID: CVE-2024-39735**		
Generation of Error Message Containing Sensitive Information	15-Jul-2024	5.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 296004. **CVE ID: CVE-2024-39737**	https://exchange.xforce.ibmcloud.com/vulnerabilities/296004, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/161
N/A	15-Jul-2024	5.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 displays version information in HTTP requests that could allow an attacker to gather information for future attacks against the system.	https://exchange.xforce.ibmcloud.com/vulnerabilities/296009, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/162

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
			IBM X-Force ID: 296009. **CVE ID: CVE-2024-39740**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	15-Jul-2024	5.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 could allow a remote attacker 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. IBM X-Force ID: 296010. **CVE ID: CVE-2024-39741**	https://exchange.xforce.ibmcloud.com/vulnerabilities/296010, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/163
Server-Side Request Forgery (SSRF)	15-Jul-2024	4.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 296008.	https://exchange.xforce.ibmcloud.com/vulnerabilities/296008, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/164

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-2024-39739		
N/A	15-Jul-2024	4.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 could allow an authenticated user to obtain sensitive information from source code that could be used in further attacks against the system. IBM X-Force ID: 295968. **CVE ID: CVE-2024-39729**	https://exchange.xforce.ibmcloud.com/vulnerabilities/295968, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/165
Product: datacap_navigator					
Affected Version(s): *					
Improper Encoding or Escaping of Output	15-Jul-2024	9.8	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 296003.	https://exchange.xforce.ibmcloud.com/vulnerabilities/296003, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/166

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
			CVE ID: CVE-2024-39736		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Jul-2024	5.4	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 295967. **CVE ID: CVE-2024-39728**	https://exchange.xforce.ibmcloud.com/vulnerabilities/295967, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/167
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Jul-2024	5.4	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a	https://exchange.xforce.ibmcloud.com/vulnerabilities/296002, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trusted session. IBM X-Force ID: 296002. **CVE ID: CVE-2024-39735**		
Generation of Error Message Containing Sensitive Information	15-Jul-2024	5.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 296004. **CVE ID: CVE-2024-39737**	https://exchange.xforce.ibmcloud.com/vulnerabilities/296004, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/169
N/A	15-Jul-2024	5.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 displays version information in HTTP requests that could allow an attacker to gather information for future attacks against the system. IBM X-Force ID: 296009. **CVE ID: CVE-2024-39740**	https://exchange.xforce.ibmcloud.com/vulnerabilities/296009, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/170
Improper Limitation	15-Jul-2024	5.3	IBM Datacap Navigator 9.1.5,	https://exchange.xforce.ibmclou	A-IBM-DATA-230724/171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			9.1.6, 9.1.7, 9.1.8, and 9.1.9 could allow a remote attacker 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. IBM X-Force ID: 296010. **CVE ID: CVE-2024-39741**	d.com/vulnerabilities/296010, https://www.ibm.com/support/pages/node/7160185	
Server-Side Request Forgery (SSRF)	15-Jul-2024	4.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 296008. **CVE ID: CVE-2024-39739**	https://exchange.xforce.ibmcloud.com/vulnerabilities/296008, https://www.ibm.com/support/pages/node/7160185	A-IBM-DATA-230724/172
N/A	15-Jul-2024	4.3	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 could allow an authenticated user	https://exchange.xforce.ibmcloud.com/vulnerabilities/295968, https://www.ibm.com/support	A-IBM-DATA-230724/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to obtain sensitive information from source code that could be used in further attacks against the system. IBM X-Force ID: 295968. **CVE ID: CVE-2024-39729**	/pages/node/7160185	
Product: i					
Affected Version(s): 7.2					
Uncontrolled Search Path Element	08-Jul-2024	7.8	IBM System Management for i 7.2, 7.3, and 7.4 could allow a local user to gain elevated privileges due to an unqualified library program call. A malicious actor could cause user-controlled code to run with administrator privilege. IBM X-Force ID: 295227. **CVE ID: CVE-2024-38330**	https://exchange.xforce.ibmcloud.com/vulnerabilities/295227, https://www.ibm.com/support/pages/node/7159615	A-IBM-I-230724/174
Affected Version(s): 7.3					
Uncontrolled Search Path Element	08-Jul-2024	7.8	IBM System Management for i 7.2, 7.3, and 7.4 could allow a local user to gain elevated privileges due to an unqualified library program call. A malicious actor could cause user-	https://exchange.xforce.ibmcloud.com/vulnerabilities/295227, https://www.ibm.com/support/pages/node/7159615	A-IBM-I-230724/175

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controlled code to run with administrator privilege. IBM X-Force ID: 295227. **CVE ID: CVE-2024-38330**		
Affected Version(s): 7.4					
Uncontrolled Search Path Element	08-Jul-2024	7.8	IBM System Management for i 7.2, 7.3, and 7.4 could allow a local user to gain elevated privileges due to an unqualified library program call. A malicious actor could cause user-controlled code to run with administrator privilege. IBM X-Force ID: 295227. **CVE ID: CVE-2024-38330**	https://exchange.xforce.ibmcloud.com/vulnerabilities/295227, https://www.ibm.com/support/pages/node/7159615	A-IBM-I-230724/176
Product: storage_virtualize					
Affected Version(s): 8.6					
Improper Authentication	08-Jul-2024	4.6	IBM FlashSystem 5300 USB ports may be usable even if the port has been disabled by the administrator. A user with physical access to the system could use the USB port to cause loss of access to data. IBM X-Force ID: 295935.	https://exchange.xforce.ibmcloud.com/vulnerabilities/295935, https://www.ibm.com/support/pages/node/7159333	A-IBM-STOR-230724/177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39723		
Vendor: icegram					
Product: email_subscribers_\&_newsletters					
Affected Version(s): * Up to (excluding) 5.7.26					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jul-2024	9.8	The Email Subscribers by Icegram Express – Email Marketing, Newsletters, Automation for WordPress & WooCommerce plugin for WordPress is vulnerable to time-based SQL Injection via the db parameter in all versions up to, and including, 5.7.25 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-2024-6172**	https://plugins.trac.wordpress.org/changeset/3107964/email-subscribers#file4	A-ICE-EMAI-230724/178

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: instawp					
Product: instawp_connect					
Affected Version(s): * Up to (excluding) 0.1.0.45					
Improper Authentication	11-Jul-2024	9.8	The InstaWP Connect – 1-click WP Staging & Migration plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 0.1.0.44. This is due to insufficient verification of the API key. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the username, and to perform a variety of other administrative tasks. NOTE: This vulnerability was partially fixed in 0.1.0.44, but was still exploitable via Cross-Site Request Forgery. **CVE ID: CVE-2024-6397**	https://plugins.trac.wordpress.org/changeset/3109305/, https://plugins.trac.wordpress.org/changeset/3114674/	A-INS-INST-230724/179
Vendor: ISC					
Product: stork					
Affected Version(s): From (including) 0.15.0 Up to (excluding) 1.15.1					

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
Improper Certificate Validation	11-Jul-2024	8.1	The TLS certificate validation code is flawed. An attacker can obtain a TLS certificate from the Stork server and use it to connect to the Stork agent. Once this connection is established with the valid certificate, the attacker can send malicious commands to a monitored service (Kea or BIND 9), possibly resulting in confidential data loss and/or denial of service. It should be noted that this vulnerability is not related to BIND 9 or Kea directly, and only customers using the Stork management tool are potentially affected. This issue affects Stork versions 0.15.0 through 1.15.0. **CVE ID: CVE-2024-28872**	https://kb.isc.org/docs/cve-2024-28872	A-ISC-STOR-230724/180
Vendor: jungo					
Product: windriver					
Affected Version(s): * Up to (excluding) 12.1.0					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver	N/A	A-JUN-WIND-230724/181

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
			before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-JUN-WIND-230724/182
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-JUN-WIND-230724/183
Affected Version(s): * Up to (excluding) 12.2.0					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code.	N/A	A-JUN-WIND-230724/184

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-25086		
Affected Version(s): * Up to (excluding) 12.5.1					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-JUN-WIND-230724/185
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-JUN-WIND-230724/186
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-JUN-WIND-230724/187
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability	N/A	A-JUN-WIND-230724/188

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
			in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**		
Affected Version(s): * Up to (excluding) 12.6.0					
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-JUN-WIND-230724/189
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-JUN-WIND-230724/190
Affected Version(s): * Up to (excluding) 12.7.0					
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error.	N/A	A-JUN-WIND-230724/191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-25087		
Affected Version(s): From (including) 6.0.0 Up to (excluding) 16.2.0					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-JUN-WIND-230724/192
Vendor: KDE					
Product: plasma-workspace					
Affected Version(s): * Up to (excluding) 5.27.11.1					
N/A	05-Jul-2024	7.8	KSmserver in KDE Plasma Workspace (aka plasma-workspace) before 5.27.11.1 and 6.x before 6.0.5.1 allows connections via ICE based purely on the host, i.e., all local connections are accepted. This allows another user on the same machine to gain access to the session manager, e.g., use the session-restore feature to execute arbitrary code as the victim (on the next boot) via	https://kde.org/info/security/advisory-20240531-1.txt	A-KDE-PLAS-230724/193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier use of the /tmp directory. **CVE ID: CVE-2024-36041**		
Affected Version(s): From (including) 6.0.0.0 Up to (excluding) 6.0.5.1					
N/A	05-Jul-2024	7.8	KSmserver in KDE Plasma Workspace (aka plasma-workspace) before 5.27.11.1 and 6.x before 6.0.5.1 allows connections via ICE based purely on the host, i.e., all local connections are accepted. This allows another user on the same machine to gain access to the session manager, e.g., use the session-restore feature to execute arbitrary code as the victim (on the next boot) via earlier use of the /tmp directory. **CVE ID: CVE-2024-36041**	https://kde.org/info/security/advisory-20240531-1.txt	A-KDE-PLAS-230724/194
Vendor: kjd					
Product: internationalized_domain_names_in_applications					
Affected Version(s): 3.6					
N/A	07-Jul-2024	7.5	A vulnerability was identified in the kjd/idna library, specifically within the `idna.encode()` function, affecting	https://github.com/kjd/idna/commit/1d365e17e10d72d0b7876316fc7b9ca0eebdd38d,	A-KJD-INTE-230724/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 3.6. The issue arises from the function's handling of crafted input strings, which can lead to quadratic complexity and consequently, a denial of service condition. This vulnerability is triggered by a crafted input that causes the `idna.encode()` function to process the input with considerable computational load, significantly increasing the processing time in a quadratic manner relative to the input size. **CVE ID: CVE-2024-3651**	https://huntr.com/bounties/93d78d07-d791-4b39-a845-cbfabc44aadb	
Vendor: kontextwork					
Product: drupal_wiki					
Affected Version(s): * Up to (excluding) 8.31.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2024	6.1	drupal-wiki.com Drupal Wiki before 8.31.1 allows XSS via comments, captions, and image titles of a Wiki page. **CVE ID: CVE-2024-34481**	N/A	A-KON-DRUP-230724/196
Vendor: kylephillips					
Product: nested_pages					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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) 3.2.8					
Cross-Site Request Forgery (CSRF)	04-Jul-2024	8.8	The Nested Pages plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.2.7. This is due to missing or incorrect nonce validation on the 'settingsPage' function and missing santization of the 'tab' parameter. This makes it possible for unauthenticated attackers to call local php files via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-5943**	https://plugins.trac.wordpress.org/changeset/3111847/	A-KYL-NEST-230724/197
Vendor: la-studioweb					
Product: element_kit_for_elementor					
Affected Version(s): * Up to (excluding) 1.3.9					
N/A	02-Jul-2024	8.8	The LA-Studio Element Kit for Elementor plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and	https://plugins.trac.wordpress.org/changeset/3108501/lastudio-element-kit/trunk/inclu	A-LA--ELEM-230724/198

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including, 1.3.8.1 via the 'map_style' parameter. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included. **CVE ID: CVE-2024-5349**	des/addons/google-maps.php	
Vendor: langchain					
Product: langchain-experimental					
Affected Version(s): From (including) 0.0.15 Up to (excluding) 0.0.21					
N/A	15-Jul-2024	8.5	Versions of the package langchain-experimental from 0.0.15 and before 0.0.21 are vulnerable to Arbitrary Code Execution when retrieving values from the database, the code will attempt to call	https://github.com/langchain-ai/langchain/commit/7b13292e3544b2f5f2bfb8a27a062ea2b0c34561	A-LAN-LANG-230724/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'eval' on all values. An attacker can exploit this vulnerability and execute arbitrary python code if they can control the input prompt and the server is configured with VectorSQLDatabaseChain. **Notes:** Impact on the Confidentiality, Integrity and Availability of the vulnerable component: Confidentiality: Code execution happens within the impacted component, in this case langchain-experimental, so all resources are necessarily accessible. Integrity: There is nothing protected by the impacted component inherently. Although anything returned from the component counts		

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as 'information' for which the trustworthiness can be compromised. Availability: The loss of availability isn't caused by the attack itself, but it happens as a result during the attacker's post-exploitation steps. Impact on the Confidentiality, Integrity and Availability of the subsequent system: As a legitimate low-privileged user of the package (PR:L) the attacker does not have more access to data owned by the package as a result of this vulnerability than they did with normal usage (e.g. can query the DB). The unintended action that one can perform by breaking out of the app environment and exfiltrating files, making remote		

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections etc. happens during the post exploitation phase in the subsequent system - in this case, the OS. AT:P: An attacker needs to be able to influence the input prompt, whilst the server is configured with the VectorSQLDatabaseChain plugin. **CVE ID: CVE-2024-21513**		
Vendor: leap13					
Product: premium_addons_for_elementor					
Affected Version(s): * Up to (excluding) 4.10.36					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jul-2024	5.4	The Premium Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Countdown widget in all versions up to, and including, 4.10.35 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above,	https://plugins.trac.wordpress.org/changeset/3111117/	A-LEA-PREM-230724/200

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
			to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-6340**		
N/A	04-Jul-2024	4.3	The Premium Addons for Elementor plugin for WordPress is vulnerable to Regular Expression Denial of Service (ReDoS) in all versions up to, and including, 4.10.35. This is due to processing user-supplied input as a regular expression. This makes it possible for authenticated attackers, with Author-level access and above, to create and query a malicious post title, resulting in slowing server resources. **CVE ID: CVE-2024-6434**	https://plugins.trac.wordpress.org/changeset/3110991/	A-LEA-PREM-230724/201
Vendor: livemeshelementor					
Product: addons_for_elementor					
Affected Version(s): * Up to (including) 8.3.7					
N/A	04-Jul-2024	8.8	The Elementor Addons by Livemesh plugin for WordPress is vulnerable to Local	N/A	A-LIV-ADDO-230724/202

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			File Inclusion in all versions up to, and including, 8.3.7 via several of the plugin's widgets through the 'style' attribute. This makes it possible for authenticated attackers, with contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included. **CVE ID: CVE-2024-2385**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jul-2024	5.4	The Elementor Addons by Livemesh plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widgets in all versions up to, and including, 8.3.7 due to insufficient input sanitization	N/A	A-LIV-ADDO-230724/203

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 on user supplied attributes. 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-2024-2926**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jul-2024	5.4	The Elementor Addons by Livemesh plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Marquee Text Widget, Testimonials Widget, and Testimonial Slider widgets in all versions up to, and including, 8.3.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary	N/A	A-LIV-ADDO-230724/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-3638**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jul-2024	5.4	The Elementor Addons by Livemesh plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Posts Grid widget in all versions up to, and including, 8.3.7 due to insufficient input sanitization and output escaping on user supplied attributes. 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-2024-3639**	N/A	A-LIV-ADDO-230724/205
Vendor: lukasbach					
Product: yana					
Affected Version(s): * Up to (including) 1.0.16					
Improper Neutralization of Input	05-Jul-2024	9.6	Lukas Bach yana =<1.0.16 is vulnerable to Cross	N/A	A-LUK-YANA-230724/206

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')			Site Scripting (XSS) via src/electron-main.ts. **CVE ID: CVE-2024-23997**		
Vendor: mattermost					
Product: mattermost					
Affected Version(s): 9.8.0					
N/A	03-Jul-2024	5.3	Mattermost versions 9.5.x <= 9.5.5 and 9.8.0, when using shared channels with multiple remote servers connected, fail to check that the remote server A requesting the server B to update the profile picture of a user is the remote that actually has the user as a local one. This allows a malicious remote A to change the profile images of users that belong to another remote server C that is connected to the server A. **CVE ID: CVE-2024-36257**	https://mattermost.com/security-updates	A-MAT-MATT-230724/207
N/A	03-Jul-2024	2.7	Mattermost versions 9.5.x <= 9.5.5 and 9.8.0 fail to sanitize the RemoteClusterFrame payloads before	https://mattermost.com/security-updates	A-MAT-MATT-230724/208

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			audit logging them which allows a high privileged attacker with access to the audit logs to read message contents. **CVE ID: CVE-2024-39353**		
Affected Version(s): From (including) 9.5.0 Up to (excluding) 9.5.6					
N/A	03-Jul-2024	6.5	Mattermost versions 9.8.0, 9.7.x <= 9.7.4, 9.6.x <= 9.6.2, 9.5.x <= 9.5.5 fail to prevent specifying a RemoteId when creating a new user which allows an attacker to specify both a remoteId and the user ID, resulting in creating a user with a user-defined user ID. This can cause some broken functionality in User Management such administrative actions against the user not working. **CVE ID: CVE-2024-6428**	https://mattermost.com/security-updates	A-MAT-MATT-230724/209
Observable Discrepancy	03-Jul-2024	5.9	Mattermost versions 9.8.x <= 9.8.0, 9.7.x <= 9.7.4, 9.6.x <= 9.6.2 and 9.5.x <= 9.5.5, when shared channels are enabled, fail to use constant time	https://mattermost.com/security-updates	A-MAT-MATT-230724/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			comparison for remote cluster tokens which allows an attacker to retrieve the remote cluster token via a timing attack during remote cluster token comparison. **CVE ID: CVE-2024-39830**		
N/A	03-Jul-2024	5.4	Mattermost versions 9.8.0, 9.7.x <= 9.7.4, 9.6.x <= 9.6.2 and 9.5.x <= 9.5.5 fail to prevent users from specifying a RemoteId for their posts which allows an attacker to specify both a remoteId and the post ID, resulting in creating a post with a user-defined post ID. This can cause some broken functionality in the channel or thread with user-defined posts **CVE ID: CVE-2024-39361**	https://mattermost.com/security-updates	A-MAT-MATT-230724/211
N/A	03-Jul-2024	5.3	Mattermost versions 9.5.x <= 9.5.5 and 9.8.0, when using shared channels with multiple remote servers connected, fail to	https://mattermost.com/security-updates	A-MAT-MATT-230724/212

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 that the remote server A requesting the server B to update the profile picture of a user is the remote that actually has the user as a local one . This allows a malicious remote A to change the profile images of users that belong to another remote server C that is connected to the server A. **CVE ID: CVE-2024-36257**		
N/A	03-Jul-2024	5.3	Mattermost versions 9.5.x <= 9.5.5 and 9.8.0 fail to properly sanitize the recipients of a webhook event which allows an attacker monitoring webhook events to retrieve the channel IDs of archived or restored channels. **CVE ID: CVE-2024-39807**	https://mattermost.com/security-updates	A-MAT-MATT-230724/213
N/A	03-Jul-2024	2.7	Mattermost versions 9.5.x <= 9.5.5 and 9.8.0 fail to sanitize the RemoteClusterFrame payloads before audit logging them	https://mattermost.com/security-updates	A-MAT-MATT-230724/214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which allows a high privileged attacker with access to the audit logs to read message contents. **CVE ID: CVE-2024-39353**		
Affected Version(s): From (including) 9.6.0 Up to (excluding) 9.6.3					
N/A	03-Jul-2024	6.5	Mattermost versions 9.8.0, 9.7.x <= 9.7.4, 9.6.x <= 9.6.2, 9.5.x <= 9.5.5 fail to prevent specifying a RemoteId when creating a new user which allows an attacker to specify both a remoteId and the user ID, resulting in creating a user with a user-defined user ID. This can cause some broken functionality in User Management such administrative actions against the user not working. **CVE ID: CVE-2024-6428**	https://mattermost.com/security-updates	A-MAT-MATT-230724/215
Observable Discrepancy	03-Jul-2024	5.9	Mattermost versions 9.8.x <= 9.8.0, 9.7.x <= 9.7.4, 9.6.x <= 9.6.2 and 9.5.x <= 9.5.5, when shared channels are enabled, fail to use constant time comparison for	https://mattermost.com/security-updates	A-MAT-MATT-230724/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote cluster tokens which allows an attacker to retrieve the remote cluster token via a timing attack during remote cluster token comparison. **CVE ID: CVE-2024-39830**		
N/A	03-Jul-2024	5.4	Mattermost versions 9.8.0, 9.7.x <= 9.7.4, 9.6.x <= 9.6.2 and 9.5.x <= 9.5.5 fail to prevent users from specifying a RemoteId for their posts which allows an attacker to specify both a remoteId and the post ID, resulting in creating a post with a user-defined post ID. This can cause some broken functionality in the channel or thread with user-defined posts **CVE ID: CVE-2024-39361**	https://mattermost.com/security-updates	A-MAT-MATT-230724/217
Affected Version(s): From (including) 9.7.0 Up to (excluding) 9.7.4					
N/A	03-Jul-2024	5.4	Mattermost versions 9.8.0, 9.7.x <= 9.7.4, 9.6.x <= 9.6.2 and 9.5.x <= 9.5.5 fail to prevent users from specifying a	https://mattermost.com/security-updates	A-MAT-MATT-230724/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RemoteId for their posts which allows an attacker to specify both a remoteId and the post ID, resulting in creating a post with a user-defined post ID. This can cause some broken functionality in the channel or thread with user-defined posts **CVE ID: CVE-2024-39361**		
Affected Version(s): From (including) 9.7.0 Up to (excluding) 9.7.5					
N/A	03-Jul-2024	6.5	Mattermost versions 9.8.0, 9.7.x <= 9.7.4, 9.6.x <= 9.6.2, 9.5.x <= 9.5.5 fail to prevent specifying a RemoteId when creating a new user which allows an attacker to specify both a remoteId and the user ID, resulting in creating a user with a user-defined user ID. This can cause some broken functionality in User Management such administrative actions against the user not working. **CVE ID: CVE-2024-6428**	https://mattermost.com/security-updates	A-MAT-MATT-230724/219

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-Jul-2024	5.9	Mattermost versions 9.8.x <= 9.8.0, 9.7.x <= 9.7.4, 9.6.x <= 9.6.2 and 9.5.x <= 9.5.5, when shared channels are enabled, fail to use constant time comparison for remote cluster tokens which allows an attacker to retrieve the remote cluster token via a timing attack during remote cluster token comparison. **CVE ID: CVE-2024-39830**	https://mattermost.com/security-updates	A-MAT-MATT-230724/220
Affected Version(s): From (including) 9.8.0 Up to (excluding) 9.8.1					
N/A	03-Jul-2024	6.5	Mattermost versions 9.8.0, 9.7.x <= 9.7.4, 9.6.x <= 9.6.2, 9.5.x <= 9.5.5 fail to prevent specifying a RemoteId when creating a new user which allows an attacker to specify both a remoteId and the user ID, resulting in creating a user with a user-defined user ID. This can cause some broken functionality in User Management such administrative	https://mattermost.com/security-updates	A-MAT-MATT-230724/221

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			actions against the user not working. **CVE ID: CVE-2024-6428**		
Observable Discrepancy	03-Jul-2024	5.9	Mattermost versions 9.8.x <= 9.8.0, 9.7.x <= 9.7.4, 9.6.x <= 9.6.2 and 9.5.x <= 9.5.5, when shared channels are enabled, fail to use constant time comparison for remote cluster tokens which allows an attacker to retrieve the remote cluster token via a timing attack during remote cluster token comparison. **CVE ID: CVE-2024-39830**	https://mattermost.com/security-updates	A-MAT-MATT-230724/222
N/A	03-Jul-2024	5.4	Mattermost versions 9.8.0, 9.7.x <= 9.7.4, 9.6.x <= 9.6.2 and 9.5.x <= 9.5.5 fail to prevent users from specifying a RemoteId for their posts which allows an attacker to specify both a remoteId and the post ID, resulting in creating a post with a user-defined post ID. This can cause some broken functionality in the channel or thread	https://mattermost.com/security-updates	A-MAT-MATT-230724/223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with user-defined posts **CVE ID: CVE-2024-39361**		
N/A	03-Jul-2024	5.3	Mattermost versions 9.5.x <= 9.5.5 and 9.8.0 fail to properly sanitize the recipients of a webhook event which allows an attacker monitoring webhook events to retrieve the channel IDs of archived or restored channels. **CVE ID: CVE-2024-39807**	https://mattermost.com/security-updates	A-MAT-MATT-230724/224
Product: mattermost_mobile					
Affected Version(s): * Up to (excluding) 2.17.0					
Improper Authentication	15-Jul-2024	6.5	Mattermost Mobile Apps versions <=2.16.0 fail to validate that the push notifications received for a server actually came from this serve that which allows a malicious server to send push notifications with another server's diagnostic ID or server URL and have them show up in mobile apps as that server's push notifications.	https://mattermost.com/security-updates	A-MAT-MATT-230724/225

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
			CVE ID: CVE-2024-39767		
Missing Initialization of Resource	15-Jul-2024	5.3	Mattermost Mobile Apps versions <=2.16.0 fail to protect against abuse of a globally shared MathJax state which allows an attacker to change the contents of a LateX post, by creating another post with specific macro definitions. **CVE ID: CVE-2024-32945**	https://mattermost.com/security-updates	A-MAT-MATT-230724/226
Vendor: Mediawiki					
Product: mediawiki					
Affected Version(s): * Up to (including) 1.42.1					
Cross-Site Request Forgery (CSRF)	07-Jul-2024	6.5	An issue was discovered in the MediaWikiChat extension for MediaWiki through 1.42.1. CSRF can occur in API modules. **CVE ID: CVE-2024-40601**	N/A	A-MED-MEDI-230724/227
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2024	4.8	An issue was discovered in the GuMaxDD skin for MediaWiki through 1.42.1. There is stored XSS via MediaWiki:Sidebar top-level menu entries.	N/A	A-MED-MEDI-230724/228

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-40599		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2024	4.8	An issue was discovered in the Metrolook skin for MediaWiki through 1.42.1. There is stored XSS via MediaWiki:Sidebar top-level menu entries. **CVE ID: CVE-2024-40600**	N/A	A-MED-MEDI-230724/229
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2024	4.8	An issue was discovered in the Tempo skin for MediaWiki through 1.42.1. There is stored XSS via MediaWiki:Sidebar top-level menu entries. **CVE ID: CVE-2024-40602**	N/A	A-MED-MEDI-230724/230
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2024	4.8	An issue was discovered in the Nimbus skin for MediaWiki through 1.42.1. There is Stored XSS via MediaWiki:Nimbus -sidebar menu and submenu entries. **CVE ID: CVE-2024-40604**	N/A	A-MED-MEDI-230724/231
Improper Neutralization of Input During Web Page Generation	07-Jul-2024	4.8	An issue was discovered in the Foreground skin for MediaWiki through 1.42.1. There is stored XSS via	N/A	A-MED-MEDI-230724/232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			MediaWiki:Sidebar top-level menu entries. **CVE ID: CVE-2024-40605**		
Insertion of Sensitive Information into Log File	07-Jul-2024	4.3	An issue was discovered in the CheckUser extension for MediaWiki through 1.42.1. The Special:Investigate feature can expose suppressed information for log events. (TimelineService does not support properly suppressing.) **CVE ID: CVE-2024-40596**	N/A	A-MED-MEDI-230724/233
Insertion of Sensitive Information into Log File	07-Jul-2024	4.3	An issue was discovered in the CheckUser extension for MediaWiki through 1.42.1. The API can expose suppressed information for log events. (The log_deleted attribute is not applied to entries.) **CVE ID: CVE-2024-40598**	N/A	A-MED-MEDI-230724/234
Cross-Site Request Forgery (CSRF)	07-Jul-2024	4.3	An issue was discovered in the ArticleRatings extension for MediaWiki through 1.42.1.	N/A	A-MED-MEDI-230724/235

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
			Special:ChangeRating allows CSRF to alter data via a GET request. **CVE ID: CVE-2024-40603**		
Vendor: mesbook					
Product: mesbook					
Affected Version(s): 20221021.03					
Allocation of Resources Without Limits or Throttling	03-Jul-2024	7.5	Uncontrolled Resource Consumption vulnerability in MESbook 20221021.03 version. An unauthenticated remote attacker can use the "message" parameter to inject a payload with dangerous JavaScript code, causing the application to loop requests on itself, which could lead to resource consumption and disable the application. **CVE ID: CVE-2024-6427**	N/A	A-MES-MESB-230724/236
N/A	03-Jul-2024	7.1	Information exposure vulnerability in MESbook 20221021.03 version, the exploitation of which could allow a local attacker, with	N/A	A-MES-MESB-230724/237

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 privileges, to access different resources by changing the API value of the application. **CVE ID: CVE-2024-6426**		
Vendor: Microsoft					
Product: .net					
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.0.7					
N/A	09-Jul-2024	7.5	.NET and Visual Studio Denial of Service Vulnerability **CVE ID: CVE-2024-38095**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38095	A-MIC-.NET-230724/238
Product: 365_apps					
Affected Version(s): -					
N/A	09-Jul-2024	8.8	Microsoft Outlook Remote Code Execution Vulnerability **CVE ID: CVE-2024-38021**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38021	A-MIC-365_-230724/239
N/A	09-Jul-2024	6.5	Microsoft Outlook Spoofing Vulnerability **CVE ID: CVE-2024-38020**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38020	A-MIC-365_-230724/240
Product: azure_cyclecloud					
Affected Version(s): From (including) 7.9.0 Up to (including) 7.9.11					
N/A	09-Jul-2024	8.8	Azure CycleCloud Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38092	A-MIC-AZUR-230724/241

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38092		
Affected Version(s): From (including) 8.0.0 Up to (including) 8.6.0					
N/A	09-Jul-2024	8.8	Azure CycleCloud Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38092**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38092	A-MIC-AZUR-230724/242
Product: azure_kinect_software_development_kit					
Affected Version(s): * Up to (excluding) 1.4.2					
N/A	09-Jul-2024	6.4	Azure Kinect SDK Remote Code Execution Vulnerability **CVE ID: CVE-2024-38086**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38086	A-MIC-AZUR-230724/243
Product: azure_network_watcher_agent					
Affected Version(s): * Up to (excluding) 1.4.3320.1					
N/A	09-Jul-2024	7.8	Azure Network Watcher VM Extension Elevation of Privilege Vulnerability **CVE ID: CVE-2024-35261**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35261	A-MIC-AZUR-230724/244
Product: defender_for_iot					
Affected Version(s): * Up to (excluding) 24.1.4					
N/A	09-Jul-2024	9.9	Microsoft Defender for IoT Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38089**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38089	A-MIC-DEFE-230724/245
Product: dynamics_365					
Affected Version(s): 9.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jul-2024	7.3	Microsoft Dynamics 365 (On-Premises) Information Disclosure Vulnerability **CVE ID: CVE-2024-30061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30061	A-MIC-DYNA-230724/246
Product: office					
Affected Version(s): 2016					
N/A	09-Jul-2024	8.8	Microsoft Outlook Remote Code Execution Vulnerability **CVE ID: CVE-2024-38021**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38021	A-MIC-OFFI-230724/247
N/A	09-Jul-2024	6.5	Microsoft Outlook Spoofing Vulnerability **CVE ID: CVE-2024-38020**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38020	A-MIC-OFFI-230724/248
Affected Version(s): 2019					
N/A	09-Jul-2024	8.8	Microsoft Outlook Remote Code Execution Vulnerability **CVE ID: CVE-2024-38021**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38021	A-MIC-OFFI-230724/249
N/A	09-Jul-2024	6.5	Microsoft Outlook Spoofing Vulnerability **CVE ID: CVE-2024-38020**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38020	A-MIC-OFFI-230724/250
Product: office_long_term_servicing_channel					
Affected Version(s): 2021					
N/A	09-Jul-2024	8.8	Microsoft Outlook Remote Code	https://msrc.microsoft.com/up	A-MIC-OFFI-230724/251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID: CVE-2024-38021**	date-guide/vulnerability/CVE-2024-38021	
N/A	09-Jul-2024	6.5	Microsoft Outlook Spoofing Vulnerability **CVE ID: CVE-2024-38020**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38020	A-MIC-OFFI-230724/252
Product: outlook					
Affected Version(s): 2016					
N/A	09-Jul-2024	6.5	Microsoft Outlook Spoofing Vulnerability **CVE ID: CVE-2024-38020**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38020	A-MIC-OUTL-230724/253
Product: sharepoint_server					
Affected Version(s): -					
N/A	09-Jul-2024	7.5	Microsoft SharePoint Server Information Disclosure Vulnerability **CVE ID: CVE-2024-32987**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-32987	A-MIC-SHAR-230724/254
Deserialization of Untrusted Data	09-Jul-2024	7.2	Microsoft SharePoint Server Remote Code Execution Vulnerability **CVE ID: CVE-2024-38023**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38023	A-MIC-SHAR-230724/255
Deserialization of Untrusted Data	09-Jul-2024	7.2	Microsoft SharePoint Server Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	A-MIC-SHAR-230724/256

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
			CVE ID: CVE-2024-38024	lity/CVE-2024-38024	
Deserialization of Untrusted Data	09-Jul-2024	7.2	Microsoft SharePoint Remote Code Execution Vulnerability **CVE ID: CVE-2024-38094**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38094	A-MIC-SHAR-230724/257
Affected Version(s): 2016					
N/A	09-Jul-2024	7.5	Microsoft SharePoint Server Information Disclosure Vulnerability **CVE ID: CVE-2024-32987**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-32987	A-MIC-SHAR-230724/258
Deserialization of Untrusted Data	09-Jul-2024	7.2	Microsoft SharePoint Server Remote Code Execution Vulnerability **CVE ID: CVE-2024-38023**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38023	A-MIC-SHAR-230724/259
Deserialization of Untrusted Data	09-Jul-2024	7.2	Microsoft SharePoint Server Remote Code Execution Vulnerability **CVE ID: CVE-2024-38024**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38024	A-MIC-SHAR-230724/260
Deserialization of Untrusted Data	09-Jul-2024	7.2	Microsoft SharePoint Remote Code Execution Vulnerability **CVE ID: CVE-2024-38094**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38094	A-MIC-SHAR-230724/261
Affected Version(s): 2019					
N/A	09-Jul-2024	7.5	Microsoft SharePoint Server	https://msrc.microsoft.com/up	A-MIC-SHAR-230724/262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability **CVE ID: CVE-2024-32987**	date-guide/vulnerability/CVE-2024-32987	
Deserialization of Untrusted Data	09-Jul-2024	7.2	Microsoft SharePoint Server Remote Code Execution Vulnerability **CVE ID: CVE-2024-38023**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38023	A-MIC-SHAR-230724/263
Deserialization of Untrusted Data	09-Jul-2024	7.2	Microsoft SharePoint Server Remote Code Execution Vulnerability **CVE ID: CVE-2024-38024**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38024	A-MIC-SHAR-230724/264
Deserialization of Untrusted Data	09-Jul-2024	7.2	Microsoft SharePoint Remote Code Execution Vulnerability **CVE ID: CVE-2024-38094**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38094	A-MIC-SHAR-230724/265
Product: visual_studio_2022					
Affected Version(s): From (including) 17.10.0 Up to (excluding) 17.10.4					
N/A	09-Jul-2024	7.5	.NET and Visual Studio Denial of Service Vulnerability **CVE ID: CVE-2024-38095**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38095	A-MIC-VISU-230724/266
Affected Version(s): From (including) 17.4.0 Up to (excluding) 17.4.21					
N/A	09-Jul-2024	7.5	.NET and Visual Studio Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	A-MIC-VISU-230724/267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38095	lity/CVE-2024-38095	
Affected Version(s): From (including) 17.6.0 Up to (excluding) 17.6.17					
N/A	09-Jul-2024	7.5	.NET and Visual Studio Denial of Service Vulnerability **CVE ID: CVE-2024-38095**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38095	A-MIC-VISU-230724/268
Affected Version(s): From (including) 17.8.0 Up to (excluding) 17.8.12					
N/A	09-Jul-2024	7.5	.NET and Visual Studio Denial of Service Vulnerability **CVE ID: CVE-2024-38095**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38095	A-MIC-VISU-230724/269
Vendor: Mitsubishielectric					
Product: cpu_module_logging_configuration_tool					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-CPU_-230724/270
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a	N/A	A-MIT-CPU_-230724/271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service (DoS). **CVE ID: CVE-2024-22106**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-CPU_-230724/272
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-CPU_-230724/273
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-CPU_-230724/274
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0	N/A	A-MIT-CPU_-230724/275

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 cause a Windows blue screen error. **CVE ID: CVE-2023-51777**		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-MIT-CPU_-230724/276
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-CPU_-230724/277
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-MIT-CPU_-230724/278

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
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-MIT-CPU_-230724/279
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-CPU_-230724/280
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-CPU_-230724/281
Product: cw_configurator					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges	N/A	A-MIT-CW_C-230724/282

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 execute arbitrary code. **CVE ID: CVE-2023-51776**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-CW_C-230724/283
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-CW_C-230724/284
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-CW_C-230724/285
N/A	02-Jul-2024	7.8	Improper privilege management in	N/A	A-MIT-CW_C-230724/286

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-CW_C-230724/287
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-MIT-CW_C-230724/288
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-CW_C-230724/289

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-MIT-CW_C-230724/290
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-MIT-CW_C-230724/291
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-CW_C-230724/292
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error.	N/A	A-MIT-CW_C-230724/293

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-25087		
Product: data_transfer					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-DATA-230724/294
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-DATA-230724/295
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-DATA-230724/296
N/A	02-Jul-2024	7.8	Improper privilege management in	N/A	A-MIT-DATA-230724/297

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-DATA-230724/298
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-DATA-230724/299
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	N/A	A-MIT-DATA-230724/300

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
			CVE ID: CVE-2023-51778		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-DATA-230724/301
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-MIT-DATA-230724/302
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-MIT-DATA-230724/303
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a	N/A	A-MIT-DATA-230724/304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Windows blue screen error. **CVE ID: CVE-2024-22105**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-DATA-230724/305
Product: data_transfer_classic					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-DATA-230724/306
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-DATA-230724/307

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-DATA-230724/308
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-DATA-230724/309
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-DATA-230724/310
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error.	N/A	A-MIT-DATA-230724/311

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2023-51777		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-MIT-DATA-230724/312
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-DATA-230724/313
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-MIT-DATA-230724/314
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a	N/A	A-MIT-DATA-230724/315

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-DATA-230724/316
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-DATA-230724/317
Product: ezsocket					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-EZSO-230724/318

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
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-EZSO-230724/319
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-EZSO-230724/320
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-EZSO-230724/321
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges	N/A	A-MIT-EZSO-230724/322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and execute arbitrary code. **CVE ID: CVE-2024-26314**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-EZSO-230724/323
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-MIT-EZSO-230724/324
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-EZSO-230724/325
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local	N/A	A-MIT-EZSO-230724/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-MIT-EZSO-230724/327
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-EZSO-230724/328
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-EZSO-230724/329
Product: fr_configurator2					
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
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-FR_C-230724/330
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-FR_C-230724/331
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-FR_C-230724/332
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges	N/A	A-MIT-FR_C-230724/333

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 execute arbitrary code. **CVE ID: CVE-2024-25088**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-FR_C-230724/334
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-FR_C-230724/335
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-MIT-FR_C-230724/336
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0	N/A	A-MIT-FR_C-230724/337

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 cause a Windows blue screen error. **CVE ID: CVE-2024-22102**		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-MIT-FR_C-230724/338
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-MIT-FR_C-230724/339
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-FR_C-230724/340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-FR_C-230724/341
Product: fr_configurator_sw3					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-FR_C-230724/342
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-FR_C-230724/343
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local	N/A	A-MIT-FR_C-230724/344

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-FR_C-230724/345
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-FR_C-230724/346
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-FR_C-230724/347
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver	N/A	A-MIT-FR_C-230724/348

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-FR_C-230724/349
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-MIT-FR_C-230724/350
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	N/A	A-MIT-FR_C-230724/351

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-22104		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-FR_C-230724/352
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-FR_C-230724/353
Product: genesis64					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-GENE-230724/354
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to	N/A	A-MIT-GENE-230724/355

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
			escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-GENE-230724/356
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-GENE-230724/357
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-GENE-230724/358

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-GENE-230724/359
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-MIT-GENE-230724/360
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-GENE-230724/361
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	N/A	A-MIT-GENE-230724/362

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-22103		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-MIT-GENE-230724/363
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-GENE-230724/364
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-GENE-230724/365
Product: gt_got1000					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local	N/A	A-MIT-GT_G-230724/366

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-GT_G-230724/367
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-GT_G-230724/368
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-GT_G-230724/369

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-GT_G-230724/370
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-GT_G-230724/371
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-MIT-GT_G-230724/372
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error.	N/A	A-MIT-GT_G-230724/373

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-22102		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-MIT-GT_G-230724/374
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-MIT-GT_G-230724/375
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-GT_G-230724/376
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a	N/A	A-MIT-GT_G-230724/377

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
			Windows blue screen error. **CVE ID: CVE-2024-25087**		
Product: gt_got2000					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-GT_G-230724/378
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-GT_G-230724/379
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-GT_G-230724/380

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-GT_G-230724/381
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-GT_G-230724/382
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-GT_G-230724/383
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	N/A	A-MIT-GT_G-230724/384

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2023-51778		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-GT_G-230724/385
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-MIT-GT_G-230724/386
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-MIT-GT_G-230724/387
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a	N/A	A-MIT-GT_G-230724/388

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
			Windows blue screen error. **CVE ID: CVE-2024-22105**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-GT_G-230724/389
Product: gt_softgot1000					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-GT_S-230724/390
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-GT_S-230724/391

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-GT_S-230724/392
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-GT_S-230724/393
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-GT_S-230724/394
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error.	N/A	A-MIT-GT_S-230724/395

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2023-51777		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-MIT-GT_S-230724/396
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-GT_S-230724/397
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-MIT-GT_S-230724/398
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a	N/A	A-MIT-GT_S-230724/399

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-GT_S-230724/400
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-GT_S-230724/401
Product: gt_softgot2000					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-GT_S-230724/402

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-GT_S-230724/403
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-GT_S-230724/404
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-GT_S-230724/405
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges	N/A	A-MIT-GT_S-230724/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and execute arbitrary code. **CVE ID: CVE-2024-26314**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-GT_S-230724/407
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-MIT-GT_S-230724/408
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-GT_S-230724/409
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local	N/A	A-MIT-GT_S-230724/410

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-MIT-GT_S-230724/411
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-GT_S-230724/412
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-GT_S-230724/413
Product: gx_developer					
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
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-GX_D-230724/414
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-GX_D-230724/415
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-GX_D-230724/416
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges	N/A	A-MIT-GX_D-230724/417

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 execute arbitrary code. **CVE ID: CVE-2024-25088**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-GX_D-230724/418
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-GX_D-230724/419
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-MIT-GX_D-230724/420
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0	N/A	A-MIT-GX_D-230724/421

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 cause a Windows blue screen error. **CVE ID: CVE-2024-22102**		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-MIT-GX_D-230724/422
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-MIT-GX_D-230724/423
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-GX_D-230724/424

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-GX_D-230724/425
Product: gx_logviewer					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-GX_L-230724/426
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-GX_L-230724/427
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local	N/A	A-MIT-GX_L-230724/428

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-GX_L-230724/429
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-GX_L-230724/430
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-GX_L-230724/431
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver	N/A	A-MIT-GX_L-230724/432

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
			before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-GX_L-230724/433
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-MIT-GX_L-230724/434
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	N/A	A-MIT-GX_L-230724/435

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-22104		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-GX_L-230724/436
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-GX_L-230724/437
Product: gx_works2					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-GX_W-230724/438
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to	N/A	A-MIT-GX_W-230724/439

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-GX_W-230724/440
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-GX_W-230724/441
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-GX_W-230724/442

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-GX_W-230724/443
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-MIT-GX_W-230724/444
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-GX_W-230724/445
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	N/A	A-MIT-GX_W-230724/446

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-22103		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-MIT-GX_W-230724/447
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-GX_W-230724/448
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-GX_W-230724/449
Product: gx_works3					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local	N/A	A-MIT-GX_W-230724/450

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
			attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-GX_W-230724/451
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-GX_W-230724/452
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-GX_W-230724/453

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-GX_W-230724/454
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-GX_W-230724/455
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-MIT-GX_W-230724/456
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error.	N/A	A-MIT-GX_W-230724/457

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-22102		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-MIT-GX_W-230724/458
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-MIT-GX_W-230724/459
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-GX_W-230724/460
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a	N/A	A-MIT-GX_W-230724/461

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
			Windows blue screen error. **CVE ID: CVE-2024-25087**		
Product: iq_works					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-IQ_W-230724/462
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-IQ_W-230724/463
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-IQ_W-230724/464

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-IQ_W-230724/465
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-IQ_W-230724/466
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-IQ_W-230724/467
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	N/A	A-MIT-IQ_W-230724/468

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
			CVE ID: CVE-2023-51778		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-IQ_W-230724/469
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-MIT-IQ_W-230724/470
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-MIT-IQ_W-230724/471
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a	N/A	A-MIT-IQ_W-230724/472

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Windows blue screen error. **CVE ID: CVE-2024-22105**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-IQ_W-230724/473
Product: mi_configurator					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-MI_C-230724/474
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-MI_C-230724/475

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
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-MI_C-230724/476
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-MI_C-230724/477
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-MI_C-230724/478
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error.	N/A	A-MIT-MI_C-230724/479

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
			CVE ID: CVE-2023-51777		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-MIT-MI_C-230724/480
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-MI_C-230724/481
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-MIT-MI_C-230724/482
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a	N/A	A-MIT-MI_C-230724/483

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
			Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-MI_C-230724/484
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-MI_C-230724/485
Product: mr_configurator					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-MR_C-230724/486

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
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-MR_C-230724/487
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-MR_C-230724/488
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-MR_C-230724/489
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges	N/A	A-MIT-MR_C-230724/490

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
			and execute arbitrary code. **CVE ID: CVE-2024-26314**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-MR_C-230724/491
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-MIT-MR_C-230724/492
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-MR_C-230724/493
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local	N/A	A-MIT-MR_C-230724/494

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-MIT-MR_C-230724/495
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-MR_C-230724/496
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-MR_C-230724/497
Product: mr_configurator2					
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
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-MR_C-230724/498
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-MR_C-230724/499
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-MR_C-230724/500
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges	N/A	A-MIT-MR_C-230724/501

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 execute arbitrary code. **CVE ID: CVE-2024-25088**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-MR_C-230724/502
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-MR_C-230724/503
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-MIT-MR_C-230724/504
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0	N/A	A-MIT-MR_C-230724/505

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 cause a Windows blue screen error. **CVE ID: CVE-2024-22102**		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-MIT-MR_C-230724/506
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-MIT-MR_C-230724/507
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-MR_C-230724/508

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-MR_C-230724/509
Product: mx_component					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-MX_C-230724/510
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-MX_C-230724/511
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local	N/A	A-MIT-MX_C-230724/512

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-MX_C-230724/513
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-MX_C-230724/514
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-MX_C-230724/515
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver	N/A	A-MIT-MX_C-230724/516

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-MX_C-230724/517
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-MIT-MX_C-230724/518
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	N/A	A-MIT-MX_C-230724/519

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-22104		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-MX_C-230724/520
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-MX_C-230724/521
Product: mx_opc_server_da\/ua					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-MX_O-230724/522
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to	N/A	A-MIT-MX_O-230724/523

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-MX_O-230724/524
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-MX_O-230724/525
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-MX_O-230724/526

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
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-MX_O-230724/527
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-MIT-MX_O-230724/528
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-MX_O-230724/529
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	N/A	A-MIT-MX_O-230724/530

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-22103		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-MIT-MX_O-230724/531
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-MX_O-230724/532
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-MX_O-230724/533
Product: numerical_control_device_communication					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local	N/A	A-MIT-NUME-230724/534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-NUME-230724/535
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-NUME-230724/536
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-NUME-230724/537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-NUME-230724/538
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-NUME-230724/539
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-MIT-NUME-230724/540
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error.	N/A	A-MIT-NUME-230724/541

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
			CVE ID: CVE-2024-22102		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-MIT-NUME-230724/542
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-MIT-NUME-230724/543
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-NUME-230724/544
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a	N/A	A-MIT-NUME-230724/545

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Windows blue screen error. **CVE ID: CVE-2024-25087**		
Product: px_developer\/monitor_tool					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-PX_D-230724/546
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-PX_D-230724/547
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-PX_D-230724/548

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-PX_D-230724/549
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-PX_D-230724/550
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-PX_D-230724/551
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	N/A	A-MIT-PX_D-230724/552

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
			CVE ID: CVE-2023-51778		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-PX_D-230724/553
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-MIT-PX_D-230724/554
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-MIT-PX_D-230724/555
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a	N/A	A-MIT-PX_D-230724/556

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Windows blue screen error. **CVE ID: CVE-2024-22105**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-PX_D-230724/557
Product: rt_toolbox3					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-RT_T-230724/558
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-RT_T-230724/559

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-RT_T-230724/560
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-RT_T-230724/561
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	A-MIT-RT_T-230724/562
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error.	N/A	A-MIT-RT_T-230724/563

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2023-51777		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-MIT-RT_T-230724/564
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-RT_T-230724/565
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	A-MIT-RT_T-230724/566
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a	N/A	A-MIT-RT_T-230724/567

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-RT_T-230724/568
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-RT_T-230724/569
Product: rt_visualbox					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	A-MIT-RT_V-230724/570

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	A-MIT-RT_V-230724/571
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	A-MIT-RT_V-230724/572
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	A-MIT-RT_V-230724/573
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges	N/A	A-MIT-RT_V-230724/574

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 execute arbitrary code. **CVE ID: CVE-2024-26314**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	A-MIT-RT_V-230724/575
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	A-MIT-RT_V-230724/576
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	A-MIT-RT_V-230724/577
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local	N/A	A-MIT-RT_V-230724/578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	A-MIT-RT_V-230724/579
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	A-MIT-RT_V-230724/580
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	A-MIT-RT_V-230724/581
Vendor: mommyheather					
Product: advanced_backups					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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) 3.6					
N/A	09-Jul-2024	5.5	Mommy Heather Advanced Backups up to v3.5.3 allows attackers to write arbitrary files via restoring a crafted back up. **CVE ID: CVE-2024-39118**	https://github.com/MommyHeather/AdvancedBackups/commit/1545f499f73bf434ed292c31121fdda8042ff5d6	A-MOM-ADVA-230724/582
Vendor: Mongodb					
Product: compass					
Affected Version(s): * Up to (excluding) 1.42.2					
Improper Control of Generation of Code ('Code Injection')	01-Jul-2024	9.8	MongoDB Compass may be susceptible to code injection due to insufficient sandbox protection settings with the usage of ejson shell parser in Compass' connection handling. This issue affects MongoDB Compass versions prior to version 1.42.2 **CVE ID: CVE-2024-6376**	https://jira.mongodb.org/browse/COMPASS-7496	A-MON-COMP-230724/583
Product: mongodb					
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.0.22					
Missing Authorization	01-Jul-2024	6.5	A command for refining a collection shard key is missing an authorization check. This may cause the command to run directly on a shard, leading to	https://jira.mongodb.org/browse/SERVER-79327	A-MON-MONG-230724/584

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 degradation of query performance, or to revealing chunk boundaries through timing side channels. This affects MongoDB Server v5.0 versions, prior to 5.0.22, MongoDB Server v6.0 versions, prior to 6.0.11 and MongoDB Server v7.0 versions prior to 7.0.3. **CVE ID: CVE-2024-6375**		
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.0.11					
Missing Authorization	01-Jul-2024	6.5	A command for refining a collection shard key is missing an authorization check. This may cause the command to run directly on a shard, leading to either degradation of query performance, or to revealing chunk boundaries through timing side channels. This affects MongoDB Server v5.0 versions, prior to 5.0.22, MongoDB Server v6.0 versions, prior to 6.0.11 and	https://jira.mongodb.org/browse/SERVER-79327	A-MON-MONG-230724/585

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MongoDB Server v7.0 versions prior to 7.0.3. **CVE ID: CVE-2024-6375**		
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.3					
Missing Authorization	01-Jul-2024	6.5	A command for refining a collection shard key is missing an authorization check. This may cause the command to run directly on a shard, leading to either degradation of query performance, or to revealing chunk boundaries through timing side channels. This affects MongoDB Server v5.0 versions, prior to 5.0.22, MongoDB Server v6.0 versions, prior to 6.0.11 and MongoDB Server v7.0 versions prior to 7.0.3. **CVE ID: CVE-2024-6375**	https://jira.mongodb.org/browse/SERVER-79327	A-MON-MONG-230724/586
Vendor: monospace					
Product: directus					
Affected Version(s): * Up to (excluding) 10.9.3					
Server-Side Request	08-Jul-2024	5	Directus is a real-time API and App dashboard for managing SQL	https://github.com/directus/directus/commit/d577b44231c0	A-MON-DIRE-230724/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			database content. There was already a reported SSRF vulnerability via file import. It was fixed by resolving all DNS names and checking if the requested IP is an internal IP address. However it is possible to bypass this security measure and execute a SSRF using redirects. Directus allows redirects when importing file from the URL and does not check the result URL. Thus, it is possible to execute a request to an internal IP, for example to 127.0.0.1. However, it is blind SSRF, because Directus also uses response interception technique to get the information about the connect from the socket directly and it does not show a response if the IP address is internal. This vulnerability is fixed in 10.9.3.	923aca99cac5770fd853801caee1, https://github.com/directus/directus/security/advisories/GHSA-8p72-rcq4-h6pw	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-39699		
Vendor: mudler					
Product: localai					
Affected Version(s): * Up to (excluding) 2.17.0					
Server-Side Request Forgery (SSRF)	06-Jul-2024	5.8	A vulnerability in the /models/apply endpoint of mudler/localai versions 2.15.0 allows for Server-Side Request Forgery (SSRF) and partial Local File Inclusion (LFI). The endpoint supports both http(s):// and file:// schemes, where the latter can lead to LFI. However, the output is limited due to the length of the error message. This vulnerability can be exploited by an attacker with network access to the LocalAI instance, potentially allowing unauthorized access to internal HTTP(s) servers and partial reading of local files. The issue is fixed in version 2.17. **CVE ID: CVE-2024-6095**	https://github.com/mudler/localai/commit/2fc6fe806b903ac0a70218b21b5c84443a1b0866	A-MUD-LOCA-230724/588
Vendor: mythemeshop					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: url_shortener					
Affected Version(s): * Up to (including) 1.0.17					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	4.8	The URL Shortener by Myhop WordPress plugin through 1.0.17 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed **CVE ID: CVE-2024-5802**	N/A	A-MYT-URL_-230724/589
Vendor: Netapp					
Product: e-series_santricity_os_controller					
Affected Version(s): From (including) 11.0.0 Up to (including) 11.70.2					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	A-NET-E-SE-230724/590

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-6387		
Product: ontap_select_deploy_administration_utility					
Affected Version(s): -					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	A-NET-ONTA-230724/591
Product: ontap_tools					
Affected Version(s): 9					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	A-NET-ONTA-230724/592

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			within a set time period. **CVE ID: CVE-2024-6387**		
Vendor: netbox					
Product: netbox					
Affected Version(s): 4.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	6.1	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/power-ports/add/. **CVE ID: CVE-2024-38972**	N/A	A-NET-NETB-230724/593
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	6.1	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/power-ports/{id}/edit/. **CVE ID: CVE-2024-40726**	N/A	A-NET-NETB-230724/594
Improper Neutralization of Input During	09-Jul-2024	6.1	A cross-site scripting (XSS) vulnerability in netbox v4.0.3	N/A	A-NET-NETB-230724/595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/console-server-ports/add/. **CVE ID: CVE-2024-40727**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	6.1	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/console-server-ports/{id}/edit/. **CVE ID: CVE-2024-40728**	N/A	A-NET-NETB-230724/596
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	6.1	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/interfaces/add/. **CVE ID: CVE-2024-40729**	N/A	A-NET-NETB-230724/597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	6.1	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/interfaces/{id}/edit/. **CVE ID: CVE-2024-40730**	N/A	A-NET-NETB-230724/598
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	6.1	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/rear-ports/{id}/edit/. **CVE ID: CVE-2024-40731**	N/A	A-NET-NETB-230724/599
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	6.1	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at	N/A	A-NET-NETB-230724/600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/dcim/rear-ports/add/. **CVE ID: CVE-2024-40732**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	6.1	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/front-ports/{id}/edit/. **CVE ID: CVE-2024-40733**	N/A	A-NET-NETB-230724/601
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	6.1	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/front-ports/add/. **CVE ID: CVE-2024-40734**	N/A	A-NET-NETB-230724/602
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	6.1	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted	N/A	A-NET-NETB-230724/603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload injected into the Name parameter at /dcim/power-outlets/{id}/edit/. **CVE ID: CVE-2024-40735**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	6.1	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/power-outlets/add. **CVE ID: CVE-2024-40736**	N/A	A-NET-NETB-230724/604
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	6.1	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/console-ports/add. **CVE ID: CVE-2024-40737**	N/A	A-NET-NETB-230724/605
Improper Neutralization of Input During Web Page	09-Jul-2024	6.1	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to	N/A	A-NET-NETB-230724/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/console-ports/{id}/edit/. **CVE ID: CVE-2024-40738**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	6.1	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/power-feeds/add. **CVE ID: CVE-2024-40739**	N/A	A-NET-NETB-230724/607
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	6.1	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/power-feeds/{id}/edit/. **CVE ID: CVE-2024-40740**	N/A	A-NET-NETB-230724/608
Improper Neutralizat	09-Jul-2024	6.1	A cross-site scripting (XSS)	N/A	A-NET-NETB-230724/609

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')			vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the circuit ID parameter at /circuits/circuits/{id}/edit/. **CVE ID: CVE-2024-40741**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	6.1	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the circuit ID parameter at /circuits/circuits/add. **CVE ID: CVE-2024-40742**	N/A	A-NET-NETB-230724/610
Vendor: oisf					
Product: suricata					
Affected Version(s): * Up to (excluding) 6.0.20					
Allocation of Resources Without Limits or Throttling	11-Jul-2024	7.5	Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine. Suricata can run out of memory when parsing	https://github.com/OISF/suricata/commit/62d5cac1b8483d5f9d2b79833a4e59f5d80129b7, https://github.com/OISF/suricata/commit/c82fa5ca0d1ce0bd8f936e0b860707	A-OIS-SURI-230724/611

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
			crafted HTTP/2 traffic. Upgrade to 6.0.20 or 7.0.6. **CVE ID: CVE-2024-38535**	a6571373b2, https://github.com/OISF/suricata/security/advisories/GHSA-cg8j-7mwm-v563	
Affected Version(s): * Up to (excluding) 7.0.6					
Allocation of Resources Without Limits or Throttling	11-Jul-2024	7.5	Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine. Crafted modbus traffic can lead to unlimited resource accumulation within a flow. Upgrade to 7.0.6. Set a limited stream.reassembly. depth to reduce the issue. **CVE ID: CVE-2024-38534**	https://github.com/OISF/suricata/commit/a753cdbe84caee3b66d0bf49b2712d29a50d67ae, https://github.com/OISF/suricata/security/advisories/GHSA-59qg-h357-69fq	A-OIS-SURI-230724/612
NULL Pointer Dereference	11-Jul-2024	7.5	Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine. A memory allocation failure due to `http.memcap` being reached leads to a NULL-ptr reference leading	https://github.com/OISF/suricata/security/advisories/GHSA-j32j-4w6g-94hh	A-OIS-SURI-230724/613

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
			to a crash. Upgrade to 7.0.6. **CVE ID: CVE-2024-38536**		
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.0.20					
Improper Check for Unusual or Exceptional Conditions	11-Jul-2024	7.5	Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine. Mishandling of multiple fragmented packets using the same IP ID value can lead to packet reassembly failure, which can lead to policy bypass. Upgrade to 7.0.6 or 6.0.20. When using af-packet, enable `defrag` to reduce the scope of the problem. **CVE ID: CVE-2024-37151**	https://github.com/OISF/suricata/commit/9d5c4273cb7e5ca65f195f7361f0d848c85180e0, https://github.com/OISF/suricata/commit/aab7f35c76721df19403a7c0c0025feae12f3b6b, https://github.com/OISF/suricata/security/advisories/GHSA-qrp7-g66m-px24	A-OIS-SURI-230724/614
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.6					
Improper Check for Unusual or Exceptional Conditions	11-Jul-2024	7.5	Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine. Mishandling of multiple	https://github.com/OISF/suricata/commit/9d5c4273cb7e5ca65f195f7361f0d848c85180e0, https://github.com/OISF/suricata/commit/aab7f35c76721df19403a7c0c0025	A-OIS-SURI-230724/615

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fragmented packets using the same IP ID value can lead to packet reassembly failure, which can lead to policy bypass. Upgrade to 7.0.6 or 6.0.20. When using af-packet, enable `defrag` to reduce the scope of the problem. **CVE ID: CVE-2024-37151**	feae12f3b6b, https://github.com/OISF/suricata/security/advisories/GHSA-qrp7-g66m-px24	
Allocation of Resources Without Limits or Throttling	11-Jul-2024	7.5	Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine. Suricata can run out of memory when parsing crafted HTTP/2 traffic. Upgrade to 6.0.20 or 7.0.6. **CVE ID: CVE-2024-38535**	https://github.com/OISF/suricata/commit/62d5cac1b8483d5f9d2b79833a4e59f5d80129b7, https://github.com/OISF/suricata/commit/c82fa5ca0d1ce0bd8f936e0b860707a6571373b2, https://github.com/OISF/suricata/security/advisories/GHSA-cg8j-7mwm-v563	A-OIS-SURI-230724/616
Vendor: Openbsd					
Product: openssh					
Affected Version(s): * Up to (excluding) 4.4					
Concurrent Execution using Shared Resource with	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html,	A-OPE-OPEN-230724/617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	https://news.ycombinator.com/item?id=40843778	
Affected Version(s): 4.4					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	A-OPE-OPEN-230724/618
Affected Version(s): 8.5					
Concurrent Execution using Shared Resource with	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html,	A-OPE-OPEN-230724/619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	https://news.ycombinator.com/item?id=40843778	
Affected Version(s): 9.8					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	A-OPE-OPEN-230724/620
Affected Version(s): From (including) 8.6 Up to (excluding) 9.8					
Concurrent Execution using Shared Resource with	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html,	A-OPE-OPEN-230724/621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	https://news.ycombinator.com/item?id=40843778	
Vendor: openfind					
Product: mail2000					
Affected Version(s): 7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Jul-2024	6.1	Openfind's Mail2000 does not properly validate email atachments, allowing unauthenticated remote attackers to inject JavaScript code within the attachment and perform Stored Cross-site scripting attacks. **CVE ID: CVE-2024-6740**	N/A	A-OPE-MAIL-230724/622
Affected Version(s): 8.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Jul-2024	6.1	Openfind's Mail2000 does not properly validate email atachments, allowing unauthenticated remote attackers to inject JavaScript	N/A	A-OPE-MAIL-230724/623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code within the attachment and perform Stored Cross-site scripting attacks. **CVE ID: CVE-2024-6740**		
Product: mailaudit					
Affected Version(s): * Up to (excluding) 6.1.7.040					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Jul-2024	6.1	The session cookie in MailGates and MailAudit from Openfind does not have the HttpOnly flag enabled, allowing remote attackers to potentially steal the session cookie via XSS. **CVE ID: CVE-2024-6739**	N/A	A-OPE-MAIL-230724/624
Product: mailgates					
Affected Version(s): * Up to (excluding) 6.1.7.040					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Jul-2024	6.1	The session cookie in MailGates and MailAudit from Openfind does not have the HttpOnly flag enabled, allowing remote attackers to potentially steal the session cookie via XSS. **CVE ID: CVE-2024-6739**	N/A	A-OPE-MAIL-230724/625
Vendor: openharmony					
Product: openharmony					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 4.0					
Out-of-bounds Read	02-Jul-2024	9.8	in OpenHarmony v4.0.0 and prior versions allow a remote attacker arbitrary code execution in pre-installed apps through out-of-bounds read and write. **CVE ID: CVE-2024-36243**	N/A	A-OPE-OPEN-230724/626
Out-of-bounds Write	02-Jul-2024	9.8	in OpenHarmony v4.0.0 and prior versions allow a remote attacker arbitrary code execution in pre-installed apps through out-of-bounds write. **CVE ID: CVE-2024-36260**	N/A	A-OPE-OPEN-230724/627
Use After Free	02-Jul-2024	9.8	in OpenHarmony v4.0.0 and prior versions allow a remote attacker arbitrary code execution in pre-installed apps through use after free. **CVE ID: CVE-2024-37030**	N/A	A-OPE-OPEN-230724/628
Out-of-bounds Write	02-Jul-2024	9.8	in OpenHarmony v4.0.0 and prior versions allow a remote attacker arbitrary code execution in pre-installed apps	N/A	A-OPE-OPEN-230724/629

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 out-of-bounds write. **CVE ID: CVE-2024-37077**		
Out-of-bounds Write	02-Jul-2024	9.8	in OpenHarmony v4.0.0 and prior versions allow a remote attacker arbitrary code execution in pre-installed apps through out-of-bounds write. **CVE ID: CVE-2024-37185**	N/A	A-OPE-OPEN-230724/630
Access of Resource Using Incompatible Type ('Type Confusion')	02-Jul-2024	3.3	in OpenHarmony v4.0.0 and prior versions allow a local attacker cause apps crash through type confusion. **CVE ID: CVE-2024-31071**	N/A	A-OPE-OPEN-230724/631
Access of Resource Using Incompatible Type ('Type Confusion')	02-Jul-2024	3.3	in OpenHarmony v4.0.0 and prior versions allow a local attacker cause apps crash through type confusion. **CVE ID: CVE-2024-36278**	N/A	A-OPE-OPEN-230724/632
Vendor: Openstack					
Product: cinder					
Affected Version(s): * Up to (excluding) 22.1.3					
N/A	05-Jul-2024	6.5	An issue was discovered in OpenStack Cinder through 24.0.0, Glance before 28.0.2, and Nova	https://launchpad.net/bugs/2059809, https://www.openwall.com/lists/oss-	A-OPE-CIND-230724/633

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
			before 29.0.3. Arbitrary file access can occur via custom QCOW2 external data. By supplying a crafted QCOW2 image that references a specific data file path, an authenticated user may convince systems to return a copy of that file's contents from the server, resulting in unauthorized access to potentially sensitive data. All Cinder and Nova deployments are affected; only Glance deployments with image conversion enabled are affected. **CVE ID: CVE-2024-32498**	security/2024/07/02/2	
Affected Version(s): 24.0.0					
N/A	05-Jul-2024	6.5	An issue was discovered in OpenStack Cinder through 24.0.0, Glance before 28.0.2, and Nova before 29.0.3. Arbitrary file access can occur via custom QCOW2 external data. By supplying a crafted	https://launchpad.net/bugs/2059809, https://www.openwall.com/lists/oss-security/2024/07/02/2	A-OPE-CIND-230724/634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QCOW2 image that references a specific data file path, an authenticated user may convince systems to return a copy of that file's contents from the server, resulting in unauthorized access to potentially sensitive data. All Cinder and Nova deployments are affected; only Glance deployments with image conversion enabled are affected. **CVE ID: CVE-2024-32498**		
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.1.1					
N/A	05-Jul-2024	6.5	An issue was discovered in OpenStack Cinder through 24.0.0, Glance before 28.0.2, and Nova before 29.0.3. Arbitrary file access can occur via custom QCOW2 external data. By supplying a crafted QCOW2 image that references a specific data file path, an authenticated user may convince	https://launchpad.net/bugs/2059809, https://www.openwall.com/lists/oss-security/2024/07/02/2	A-OPE-CIND-230724/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			systems to return a copy of that file's contents from the server, resulting in unauthorized access to potentially sensitive data. All Cinder and Nova deployments are affected; only Glance deployments with image conversion enabled are affected. **CVE ID: CVE-2024-32498**		
Product: glance					
Affected Version(s): * Up to (excluding) 26.0.1					
N/A	05-Jul-2024	6.5	An issue was discovered in OpenStack Cinder through 24.0.0, Glance before 28.0.2, and Nova before 29.0.3. Arbitrary file access can occur via custom QCOW2 external data. By supplying a crafted QCOW2 image that references a specific data file path, an authenticated user may convince systems to return a copy of that file's contents from the server, resulting in unauthorized	https://launchpad.net/bugs/2059809, https://www.openwall.com/lists/oss-security/2024/07/02/2	A-OPE-GLAN-230724/636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to potentially sensitive data. All Cinder and Nova deployments are affected; only Glance deployments with image conversion enabled are affected. **CVE ID: CVE-2024-32498**		
Affected Version(s): 27.0.0					
N/A	05-Jul-2024	6.5	An issue was discovered in OpenStack Cinder through 24.0.0, Glance before 28.0.2, and Nova before 29.0.3. Arbitrary file access can occur via custom QCOW2 external data. By supplying a crafted QCOW2 image that references a specific data file path, an authenticated user may convince systems to return a copy of that file's contents from the server, resulting in unauthorized access to potentially sensitive data. All Cinder and Nova deployments are affected; only	https://launchpad.net/bugs/2059809, https://www.openwall.com/lists/oss-security/2024/07/02/2	A-OPE-GLAN-230724/637

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Glance deployments with image conversion enabled are affected. **CVE ID: CVE-2024-32498**		
Affected Version(s): From (including) 28.0.0 Up to (excluding) 28.0.2					
N/A	05-Jul-2024	6.5	An issue was discovered in OpenStack Cinder through 24.0.0, Glance before 28.0.2, and Nova before 29.0.3. Arbitrary file access can occur via custom QCOW2 external data. By supplying a crafted QCOW2 image that references a specific data file path, an authenticated user may convince systems to return a copy of that file's contents from the server, resulting in unauthorized access to potentially sensitive data. All Cinder and Nova deployments are affected; only Glance deployments with image conversion enabled are affected.	https://launchpad.net/bugs/2059809, https://www.openwall.com/lists/oss-security/2024/07/02/2	A-OPE-GLAN-230724/638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-32498		
Product: nova					
Affected Version(s): * Up to (excluding) 27.3.1					
N/A	05-Jul-2024	6.5	An issue was discovered in OpenStack Cinder through 24.0.0, Glance before 28.0.2, and Nova before 29.0.3. Arbitrary file access can occur via custom QCOW2 external data. By supplying a crafted QCOW2 image that references a specific data file path, an authenticated user may convince systems to return a copy of that file's contents from the server, resulting in unauthorized access to potentially sensitive data. All Cinder and Nova deployments are affected; only Glance deployments with image conversion enabled are affected. **CVE ID: CVE-2024-32498**	https://launchpad.net/bugs/2059809, https://www.openwall.com/lists/oss-security/2024/07/02/2	A-OPE-NOVA-230724/639
Affected Version(s): From (including) 28.0.0 Up to (excluding) 28.1.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Jul-2024	6.5	An issue was discovered in OpenStack Cinder through 24.0.0, Glance before 28.0.2, and Nova before 29.0.3. Arbitrary file access can occur via custom QCOW2 external data. By supplying a crafted QCOW2 image that references a specific data file path, an authenticated user may convince systems to return a copy of that file's contents from the server, resulting in unauthorized access to potentially sensitive data. All Cinder and Nova deployments are affected; only Glance deployments with image conversion enabled are affected. **CVE ID: CVE-2024-32498**	https://launchpad.net/bugs/2059809, https://www.openwall.com/lists/oss-security/2024/07/02/2	A-OPE-NOVA-230724/640
Affected Version(s): From (including) 29.0.0 Up to (excluding) 29.0.3					
N/A	05-Jul-2024	6.5	An issue was discovered in OpenStack Cinder through 24.0.0, Glance before 28.0.2, and Nova	https://launchpad.net/bugs/2059809, https://www.openwall.com/lists/oss-	A-OPE-NOVA-230724/641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 29.0.3. Arbitrary file access can occur via custom QCOW2 external data. By supplying a crafted QCOW2 image that references a specific data file path, an authenticated user may convince systems to return a copy of that file's contents from the server, resulting in unauthorized access to potentially sensitive data. All Cinder and Nova deployments are affected; only Glance deployments with image conversion enabled are affected. **CVE ID: CVE-2024-32498**	security/2024/07/02/2	
Vendor: Openvpn					
Product: openvpn					
Affected Version(s): * Up to (excluding) 2.5.10					
Unrestricted Upload of File with Dangerous Type	08-Jul-2024	9.8	OpenVPN plug-ins on Windows with OpenVPN 2.6.9 and earlier could be loaded from any directory, which allows an attacker to load an arbitrary plug-in which can	https://community.openvpn.net/openvpn/wiki/CVE-2024-27903, https://openvpn.net/security-advisory/ovpnx-vulnerability-	A-OPE-OPEN-230724/642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used to interact with the privileged OpenVPN interactive service. **CVE ID: CVE-2024-27903**	cve-2024-27903-cve-2024-27459-cve-2024-24974/	
Out-of-bounds Write	08-Jul-2024	7.8	The interactive service in OpenVPN 2.6.9 and earlier allows an attacker to send data causing a stack overflow which can be used to execute arbitrary code with more privileges. **CVE ID: CVE-2024-27459**	https://community.openvpn.net/openvpn/wiki/CVE-2024-27459, https://openvpn.net/security-advisory/ovpnx-vulnerability-cve-2024-27903-cve-2024-27459-cve-2024-24974/	A-OPE-OPEN-230724/643
N/A	08-Jul-2024	7.5	The interactive service in OpenVPN 2.6.9 and earlier allows the OpenVPN service pipe to be accessed remotely, which allows a remote attacker to interact with the privileged OpenVPN interactive service. **CVE ID: CVE-2024-24974**	https://community.openvpn.net/openvpn/wiki/CVE-2024-24974, https://openvpn.net/security-advisory/ovpnx-vulnerability-cve-2024-27903-cve-2024-27459-cve-2024-24974/	A-OPE-OPEN-230724/644
Affected Version(s): From (including) 2.6.0 Up to (excluding) 2.6.10					
Unrestricted Upload of File with Dangerous Type	08-Jul-2024	9.8	OpenVPN plug-ins on Windows with OpenVPN 2.6.9 and earlier could be loaded from any directory, which allows an attacker	https://community.openvpn.net/openvpn/wiki/CVE-2024-27903, https://openvpn.net/security-	A-OPE-OPEN-230724/645

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 load an arbitrary plug-in which can be used to interact with the privileged OpenVPN interactive service. **CVE ID: CVE-2024-27903**	advisory/ovpnx-vulnerability-cve-2024-27903-cve-2024-27459-cve-2024-24974/	
Out-of-bounds Write	08-Jul-2024	7.8	The interactive service in OpenVPN 2.6.9 and earlier allows an attacker to send data causing a stack overflow which can be used to execute arbitrary code with more privileges. **CVE ID: CVE-2024-27459**	https://community.openvpn.net/openvpn/wiki/CVE-2024-27459, https://openvpn.net/security-advisory/ovpnx-vulnerability-cve-2024-27903-cve-2024-27459-cve-2024-24974/	A-OPE-OPEN-230724/646
N/A	08-Jul-2024	7.5	The interactive service in OpenVPN 2.6.9 and earlier allows the OpenVPN service pipe to be accessed remotely, which allows a remote attacker to interact with the privileged OpenVPN interactive service. **CVE ID: CVE-2024-24974**	https://community.openvpn.net/openvpn/wiki/CVE-2024-24974, https://openvpn.net/security-advisory/ovpnx-vulnerability-cve-2024-27903-cve-2024-27459-cve-2024-24974/	A-OPE-OPEN-230724/647
Vendor: Otrs					
Product: otrs					
Affected Version(s): From (including) 8.0.0 Up to (excluding) 2024.5.2					
N/A	15-Jul-2024	7.5	An incorrect privilege	https://otrs.com/release-	A-OTR-OTRS-230724/648

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
			assignment vulnerability in the inline editing functionality of OTRS can lead to privilege escalation. This flaw allows an agent with read-only permissions to gain full access to a ticket. This issue arises in very rare instances when an admin has previously enabled the setting 'RequiredLock' of 'AgentFrontend::Ticket::InlineEditing::Property###Watch' in the system configuration.This issue affects OTRS: * 8.0.X * 2023.X * from 2024.X through 2024.4.x **CVE ID: CVE-2024-23794**	notes/otrs-security-advisory-2024-06/	
N/A	15-Jul-2024	5.3	Improper filtering of fields when using the export function in the ticket overview of the external interface in OTRS could allow an authorized user	https://otrs.com/release-notes/otrs-security-advisory-2024-07/	A-OTR-OTRS-230724/649

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 download a list of tickets containing information about tickets of other customers. The problem only occurs if the TicketSearchLegacyEngine has been disabled by the administrator. This issue affects OTRS: 8.0.X, 2023.X, from 2024.X through 2024.4.x **CVE ID: CVE-2024-6540**		
Vendor: oxilab					
Product: image_hover_effects_for_elementor_with_lightbox_and_flipbox					
Affected Version(s): * Up to (including) 3.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in biplob018 Image Hover Effects - Caption Hover with Carousel allows Stored XSS.This issue affects Image Hover Effects - Caption Hover with Carousel: from n/a through 3.0.2.	N/A	A-OXI-IMAG-230724/650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-37546		
Vendor: parorrey					
Product: json_api_user					
Affected Version(s): * Up to (excluding) 3.9.4					
N/A	11-Jul-2024	9.8	The JSON API User plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 3.9.3. This is due to improper controls on custom user meta fields. This makes it possible for unauthenticated attackers to register as administrators on the site. The plugin requires the JSON API plugin to also be installed. **CVE ID: CVE-2024-6624**	https://plugins.trac.wordpress.org/changeset/3115185/	A-PAR-JSON-230724/651
Vendor: payflex					
Product: payment_gateway					
Affected Version(s): * Up to (including) 2.5.0					
Missing Authorization	11-Jul-2024	5.3	The Payflex Payment Gateway plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the	N/A	A-PAY-PAYM-230724/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payment_callback() function in all versions up to, and including, 2.5.0. This makes it possible for unauthenticated attackers to update the status of orders, which can potentially lead to revenue loss. **CVE ID: CVE-2024-0619**		
Vendor: personal-management-system					
Product: personal_management_system					
Affected Version(s): 1.4.64					
Server-Side Request Forgery (SSRF)	05-Jul-2024	9.8	Volmarg Personal Management System 1.4.64 is vulnerable to SSRF (Server Side Request Forgery) via uploading a SVG file. The server can make unintended HTTP and DNS requests to a server that the attacker controls. **CVE ID: CVE-2024-29319**	N/A	A-PER-PERS-230724/653
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2024	5.4	Volmarg Personal Management System 1.4.64 is vulnerable to stored cross site scripting (XSS) via upload of a SVG file with embedded javascript code.	N/A	A-PER-PERS-230724/654

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-29318		
Vendor: Phpvibe					
Product: phpvibe					
Affected Version(s): From (including) 11.0.3 Up to (including) 11.0.46					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Jul-2024	9.8	Directory Travel in PHPVibe v11.0.46 due to incomplete blacklist checksums and directory checks, which can lead to code execution via writing specific statements to .htaccess and code to a file with a .png suffix. **CVE ID: CVE-2024-39171**	N/A	A-PHP-PHPV-230724/655
Vendor: Playsms					
Product: playsms					
Affected Version(s): 1.4.3					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-Jul-2024	8.8	A vulnerability was found in playSMS 1.4.3. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /index.php?app=main&inc=feature_firewall&op=firewall_list of the component Template Handler. The manipulation of the argument IP	N/A	A-PLA-PLAY-230724/656

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 with the input {{`id`} leads to injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-270277 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-6469**		
Vendor: plugin-devs					
Product: blog\,_posts_and_category_filter_for_elementor					
Affected Version(s): * Up to (excluding) 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	5.4	The Blog, Posts and Category Filter for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Post and Category Filter widget in all versions up to, and including, 1.0.3 due to insufficient input sanitization and output escaping on user supplied 'post_types' attribute. This makes it possible	https://plugins.trac.wordpress.org/browser/blog-posts-and-category-for-elementor/trunk/widgets/post-category-filter.php#L885	A-PLU-BLOG-230724/657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2024-4667**		
Vendor: posimyth					
Product: the_plus_addons_for_elementor					
Affected Version(s): * Up to (excluding) 5.6.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jul-2024	5.4	The The Plus Addons for Elementor – Elementor Addons, Page Templates, Widgets, Mega Menu, WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Countdown' widget in all versions up to, and including, 5.6.1 due to insufficient input sanitization and output escaping on user supplied 'text_days' attribute. This makes it possible for authenticated attackers, with contributor-level	N/A	A-POS-THE_-230724/658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-4482**		
Vendor: publiccms					
Product: publiccms					
Affected Version(s): * Up to (including) 4.0.202302.e					
Server-Side Request Forgery (SSRF)	12-Jul-2024	8.8	PublicCMS v4.0.202302.e was discovered to contain a Server-Side Request Forgery (SSRF) via the component /admin/ueditor?action=catchimage. **CVE ID: CVE-2024-40543**	N/A	A-PUB-PUBL-230724/659
Server-Side Request Forgery (SSRF)	12-Jul-2024	8.8	PublicCMS v4.0.202302.e was discovered to contain a Server-Side Request Forgery (SSRF) via the component /admin/#maintenance_sysTask/edit. **CVE ID: CVE-2024-40544**	N/A	A-PUB-PUBL-230724/660
Unrestricted Upload of File with Dangerous Type	12-Jul-2024	8.8	An arbitrary file upload vulnerability in the component /admin/cmsWebFile/doUpload of PublicCMS	N/A	A-PUB-PUBL-230724/661

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.0.202302.e allows attackers to execute arbitrary code via uploading a crafted file. **CVE ID: CVE-2024-40545**		
Unrestricted Upload of File with Dangerous Type	12-Jul-2024	8.8	An arbitrary file upload vulnerability in the component /admin/cmsWebFile/save of PublicCMS v4.0.202302.e allows attackers to execute arbitrary code via uploading a crafted file. **CVE ID: CVE-2024-40546**	N/A	A-PUB-PUBL-230724/662
Unrestricted Upload of File with Dangerous Type	12-Jul-2024	8.8	An arbitrary file upload vulnerability in the component /admin/cmsTemplate/save of PublicCMS v4.0.202302.e allows attackers to execute arbitrary code via uploading a crafted file. **CVE ID: CVE-2024-40548**	N/A	A-PUB-PUBL-230724/663
Unrestricted Upload of File with Dangerous Type	12-Jul-2024	8.8	An arbitrary file upload vulnerability in the component /admin/cmsTemplate/savePlace of PublicCMS	N/A	A-PUB-PUBL-230724/664

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.0.202302.e allows attackers to execute arbitrary code via uploading a crafted file. **CVE ID: CVE-2024-40549**		
Unrestricted Upload of File with Dangerous Type	12-Jul-2024	8.8	An arbitrary file upload vulnerability in the component /admin/cmsTemplate/savePlaceMetaData of Public CMS v.4.0.202302.e allows attackers to execute arbitrary code via uploading a crafted file. **CVE ID: CVE-2024-40550**	N/A	A-PUB-PUBL-230724/665
Unrestricted Upload of File with Dangerous Type	12-Jul-2024	8.8	An arbitrary file upload vulnerability in the component /admin/cmsTemplate/doUpload of PublicCMS v4.0.202302.e allows attackers to execute arbitrary code via uploading a crafted file. **CVE ID: CVE-2024-40551**	N/A	A-PUB-PUBL-230724/666
N/A	12-Jul-2024	8.8	PublicCMS v4.0.202302.e was discovered to contain a remote commande execution (RCE) vulnerability via	N/A	A-PUB-PUBL-230724/667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the cmdarray parameter at /site/ScriptComponent.java. **CVE ID: CVE-2024-40552**		
N/A	12-Jul-2024	6.5	PublicCMS v4.0.202302.e was discovered to contain an arbitrary file content replacement vulnerability via the component /admin/cmsTemplate/replace. **CVE ID: CVE-2024-40547**	N/A	A-PUB-PUBL-230724/668
Vendor: Qemu					
Product: qemu					
Affected Version(s): -					
Out-of-bounds Read	05-Jul-2024	6.8	A flaw was found in the virtio-net device in QEMU. When enabling the RSS feature on the virtio-net network card, the indirections_table data within RSS becomes controllable. Setting excessively large values may cause an index out-of-bounds issue, potentially resulting in heap overflow access. This flaw allows a privileged user in	N/A	A-QEM-QEMU-230724/669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the guest to crash the QEMU process on the host. **CVE ID: CVE-2024-6505**		
Vendor: QT					
Product: qt					
Affected Version(s): * Up to (excluding) 5.15.18					
Time-of-check Time-of-use (TOCTOU) Race Condition	04-Jul-2024	5.9	An issue was discovered in HTTP2 in Qt before 5.15.18, 6.x before 6.2.13, 6.3.x through 6.5.x before 6.5.7, and 6.6.x through 6.7.x before 6.7.3. Code to make security-relevant decisions about an established connection may execute too early, because the encrypted() signal has not yet been emitted and processed.. **CVE ID: CVE-2024-39936**	https://codereview.qt-project.org/c/qt/qtbase/+/571601	A-QT-QT-230724/670
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.2.13					
Time-of-check Time-of-use (TOCTOU) Race Condition	04-Jul-2024	5.9	An issue was discovered in HTTP2 in Qt before 5.15.18, 6.x before 6.2.13, 6.3.x through 6.5.x before 6.5.7, and 6.6.x through 6.7.x before 6.7.3. Code to make security-	https://codereview.qt-project.org/c/qt/qtbase/+/571601	A-QT-QT-230724/671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			relevant decisions about an established connection may execute too early, because the encrypted() signal has not yet been emitted and processed.. **CVE ID: CVE-2024-39936**		
Affected Version(s): From (including) 6.3.0 Up to (excluding) 6.5.7					
Time-of-check Time-of-use (TOCTOU) Race Condition	04-Jul-2024	5.9	An issue was discovered in HTTP2 in Qt before 5.15.18, 6.x before 6.2.13, 6.3.x through 6.5.x before 6.5.7, and 6.6.x through 6.7.x before 6.7.3. Code to make security-relevant decisions about an established connection may execute too early, because the encrypted() signal has not yet been emitted and processed.. **CVE ID: CVE-2024-39936**	https://codereview.qt-project.org/c/qt/qtbase/+/571601	A-QT-QT-230724/672
Affected Version(s): From (including) 6.6.0 Up to (excluding) 6.7.3					
Time-of-check Time-of-use (TOCTOU)	04-Jul-2024	5.9	An issue was discovered in HTTP2 in Qt before 5.15.18, 6.x before 6.2.13, 6.3.x through 6.5.x	https://codereview.qt-project.org/c/qt/qtbase/+/571601	A-QT-QT-230724/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			before 6.5.7, and 6.6.x through 6.7.x before 6.7.3. Code to make security-relevant decisions about an established connection may execute too early, because the encrypted() signal has not yet been emitted and processed.. **CVE ID: CVE-2024-39936**		
Vendor: quivr					
Product: quivr					
Affected Version(s): * Up to (including) 0.0.281					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2024	5.4	A stored cross-site scripting (XSS) vulnerability exists in the 'Upload Knowledge' feature of stangirard/quivr, affecting the latest version. Users can upload files via URL, which allows the insertion of malicious JavaScript payloads. These payloads are stored on the server and executed whenever any user clicks on a link containing the payload, leading to potential data theft, session hijacking,	N/A	A-QUI-QUIV-230724/674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and reputation damage. **CVE ID: CVE-2024-6229**		
Vendor: radiustheme					
Product: the_post_grid					
Affected Version(s): * Up to (excluding) 7.7.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-2024	5.4	The The Post Grid – Shortcode, Gutenberg Blocks and Elementor Addon for Post Grid plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the section title tag attribute in all versions up to, and including, 7.7.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-1427**	https://plugins.trac.wordpress.org/changeset/3080313/#file347	A-RAD-THE_-230724/675
Vendor: rankmath					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: seo					
Affected Version(s): * Up to (excluding) 1.0.219					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-2024	5.4	The Rank Math SEO WordPress plugin before 1.0.219 does not sanitise and escape some of its settings, which could allow users with access to the General Settings (by default admin, however such access can be given to lower roles via the Role Manager feature of the Rank Math SEO WordPress plugin before 1.0.219) to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID: CVE-2024-4627**	N/A	A-RAN-SEO-230724/676
Vendor: Realtek					
Product: rtl819x_jungle_software_development_kit					
Affected Version(s): 3.4.11					
Cross-Site Request Forgery (CSRF)	08-Jul-2024	8.8	A cross-site request forgery (csrf) vulnerability exists in the boa CSRF protection functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted	N/A	A-REA-RTL8-230724/677

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
			network request can lead to CSRF. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID: CVE-2023-47677**		
Improper Verification of Cryptographic Signature	08-Jul-2024	7.2	A firmware update vulnerability exists in the boa formUpload functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted network packets can lead to arbitrary firmware update. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID: CVE-2023-34435**	N/A	A-REA-RTL8-230724/678
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa formRoute functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send an HTTP request to	N/A	A-REA-RTL8-230724/679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trigger this vulnerability. **CVE ID: CVE-2023-41251**		
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa setRepeaterSsid functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID: CVE-2023-45215**	N/A	A-REA-RTL8-230724/680
Integer Overflow or Wraparound	08-Jul-2024	7.2	An integer overflow vulnerability exists in the boa updateConfigIntoFlash functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID: CVE-2023-45742**	N/A	A-REA-RTL8-230724/681

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
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa set_RadvdPrefixParam functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID: CVE-2023-47856**	N/A	A-REA-RTL8-230724/682
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa formDnsv6 functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID: CVE-2023-48270**	N/A	A-REA-RTL8-230724/683
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa formFilter	N/A	A-REA-RTL8-230724/684

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID: CVE-2023-49073**		
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa rollback_control_code functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID: CVE-2023-49595**	N/A	A-REA-RTL8-230724/685
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to	N/A	A-REA-RTL8-230724/686

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution. An attacker can send a series of HTTP requests to trigger this vulnerability. **CVE ID: CVE-2023-49867**		
Out-of-bounds Write	08-Jul-2024	7.2	Two stack-based buffer overflow vulnerabilities exist in the boa set_RadvdInterface Param functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `interfacename` request's parameter. **CVE ID: CVE-2023-50239**	N/A	A-REA-RTL8-230724/687
Out-of-bounds Write	08-Jul-2024	7.2	Two stack-based buffer overflow vulnerabilities exist in the boa set_RadvdInterface Param functionality of Realtek rtl819x	N/A	A-REA-RTL8-230724/688

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
			Jungle SDK v3.4.11. A specially crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `AdvDefaultPreference` request's parameter. **CVE ID: CVE-2023-50240**		
Out-of-bounds Write	08-Jul-2024	7.2	Two stack-based buffer overflow vulnerabilities exist in the boa formIpQoS functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `comment` request's parameter.	N/A	A-REA-RTL8-230724/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2023-50243		
Out-of-bounds Write	08-Jul-2024	7.2	Two stack-based buffer overflow vulnerabilities exist in the boa formIpQoS functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `entry_name` request's parameter. **CVE ID: CVE-2023-50244**	N/A	A-REA-RTL8-230724/690
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa getInfo functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send a series of HTTP requests to trigger this vulnerability.	N/A	A-REA-RTL8-230724/691

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2023-50330		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jul-2024	7.2	Three os command injection vulnerabilities exist in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary command execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This command injection is related to the `targetAPSsid` request's parameter. **CVE ID: CVE-2023-50381**	N/A	A-REA-RTL8-230724/692
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jul-2024	7.2	Three os command injection vulnerabilities exist in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary command execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This	N/A	A-REA-RTL8-230724/693

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 is related to the `peerPin` request's parameter. **CVE ID: CVE-2023-50382**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jul-2024	7.2	Three os command injection vulnerabilities exist in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary command execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This command injection is related to the `localPin` request's parameter. **CVE ID: CVE-2023-50383**	N/A	A-REA-RTL8-230724/694
Out-of-bounds Write	08-Jul-2024	7.2	A heap-based buffer overflow vulnerability exists in the configuration file mib_init_value_array functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted .dat file can lead to arbitrary code execution. An attacker can upload	N/A	A-REA-RTL8-230724/695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a malicious file to trigger this vulnerability. **CVE ID: CVE-2024-21778**		
Vendor: Redhat					
Product: directory_server					
Affected Version(s): 12.0					
N/A	09-Jul-2024	6.5	A flaw was found in the 389 Directory Server. This flaw allows an unauthenticated user to cause a systematic server crash while sending a specific extended search request, leading to a denial of service. **CVE ID: CVE-2024-6237**	https://access.redhat.com/security/cve/CVE-2024-6237	A-RED-DIRE-230724/696
Product: openshift_container_platform					
Affected Version(s): 4.0					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	A-RED-OPEN-230724/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			within a set time period. **CVE ID: CVE-2024-6387**		
Vendor: Rejetto					
Product: http_file_server					
Affected Version(s): * Up to (excluding) 0.52.10					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Jul-2024	8.8	rejetto HFS (aka HTTP File Server) 3 before 0.52.10 on Linux, UNIX, and macOS allows OS command execution by remote authenticated users (if they have Upload permissions). This occurs because a shell is used to execute df (i.e., with execSync instead of spawnSync in child_process in Node.js). **CVE ID: CVE-2024-39943**	https://github.com/rejetto/hfs/commit/305381bd36eee074fb238b64302a252668daad1d, https://github.com/rejetto/hfs/compare/v0.52.9...v0.52.10	A-REJ-HTTP-230724/698
Vendor: Samsung					
Product: flow					
Affected Version(s): * Up to (excluding) 4.9.13.0					
N/A	02-Jul-2024	3.3	Improper verification of intent by broadcast receiver vulnerability in Samsung Flow prior to version 4.9.13.0 allows local attackers to	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=07	A-SAM-FLOW-230724/699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			copy image files to external storage. **CVE ID: CVE-2024-34600**		
Product: galaxystore					
Affected Version(s): * Up to (excluding) 4.5.81.0					
N/A	02-Jul-2024	5.3	Improper verification of intent by broadcast receiver vulnerability in GalaxyStore prior to version 4.5.81.0 allows local attackers to launch unexported activities of GalaxyStore. **CVE ID: CVE-2024-34601**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=07	A-SAM-GALA-230724/700
Product: health					
Affected Version(s): * Up to (excluding) 6.27.0.113					
N/A	02-Jul-2024	3.3	Improper input validation in Samsung Health prior to version 6.27.0.113 allows local attackers to write arbitrary document files to the sandbox of Samsung Health. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34597**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=07	A-SAM-HEAL-230724/701
Product: smartthings					
Affected Version(s): * Up to (excluding) 1.8.17					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	7.5	Improper authentication in SmartThings prior to version 1.8.17 allows remote attackers to bypass the expiration date for members set by the owner. **CVE ID: CVE-2024-34596**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=07	A-SAM-SMAR-230724/702
Product: tips					
Affected Version(s): * Up to (excluding) 6.2.9.4					
N/A	02-Jul-2024	3.3	Improper input validation in Tips prior to version 6.2.9.4 in Android 14 allows local attacker to send broadcast with Tips' privilege. **CVE ID: CVE-2024-34599**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=07	A-SAM-TIPS-230724/703
Vendor: Schneider-electric					
Product: ecostruxure_foxboro_dcs_control_core_services					
Affected Version(s): * Up to (including) 9.8					
Improper Input Validation	11-Jul-2024	7.8	CWE-20: Improper Input Validation vulnerability exists that could cause local denial-of-service, privilege escalation, and potentially kernel execution when a malicious actor with local user	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-191-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-191-02.pdf	A-SCH-ECOS-230724/704

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 crafts a script/program using an IOCTL call in the Foxboro.sys driver. **CVE ID: CVE-2024-5681**		
Out-of-bounds Write	11-Jul-2024	7.1	CWE-787: Out-of-Bounds Write vulnerability exists that could cause local denial-of-service, or kernel memory leak when a malicious actor with local user access crafts a script/program using an IOCTL call in the Foxboro.sys driver. **CVE ID: CVE-2024-5679**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-191-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-191-02.pdf	A-SCH-ECOS-230724/705
Improper Validation of Array Index	11-Jul-2024	5.5	CWE-129: Improper Validation of Array Index vulnerability exists that could cause local denial-of-service when a malicious actor with local user access crafts a script/program using an IOCTL call in the Foxboro.sys driver. **CVE ID: CVE-2024-5680**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-191-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-191-02.pdf	A-SCH-ECOS-230724/706
Product: foxrtu_station					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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) 9.3.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Jul-2024	7.8	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could result in remote code execution when an authenticated user executes a saved project file that has been tampered by a malicious actor. **CVE ID: CVE-2024-2602**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-191-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-191-03.pdf	A-SCH-FOXR-230724/707
Vendor: seacms					
Product: seacms					
Affected Version(s): * Up to (including) 12.9					
N/A	05-Jul-2024	9.8	An issue was discovered in SeaCMS <=12.9 which allows remote attackers to execute arbitrary code via admin_ping.php. **CVE ID: CVE-2024-39028**	N/A	A-SEA-SEAC-230724/708
Affected Version(s): 12.9					
N/A	12-Jul-2024	8.8	SeaCMS 12.9 has a remote code execution vulnerability. The vulnerability is caused by admin_weixin.php	N/A	A-SEA-SEAC-230724/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			directly splicing and writing the user input data into weixin.php without processing it, which allows authenticated attackers to exploit the vulnerability to execute arbitrary commands and obtain system permissions. **CVE ID: CVE-2024-40518**		
N/A	12-Jul-2024	8.8	SeaCMS 12.9 has a remote code execution vulnerability. The vulnerability is caused by admin_smtp.php directly splicing and writing the user input data into weixin.php without processing it, which allows authenticated attackers to exploit the vulnerability to execute arbitrary commands and obtain system permissions. **CVE ID: CVE-2024-40519**	N/A	A-SEA-SEAC-230724/710
N/A	12-Jul-2024	8.8	SeaCMS 12.9 has a remote code execution vulnerability. The vulnerability is caused by	N/A	A-SEA-SEAC-230724/711

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin_config_mark .php directly splicing and writing the user input data into inc_photowatermar k_config.php without processing it, which allows authenticated attackers to exploit the vulnerability to execute arbitrary commands and obtain system permissions. **CVE ID: CVE-2024-40520**		
N/A	12-Jul-2024	8.8	SeaCMS 12.9 has a remote code execution vulnerability. The vulnerability is due to the fact that although admin_template.ph p imposes certain restrictions on the edited file, attackers can still bypass the restrictions and write code in some way, allowing authenticated attackers to exploit the vulnerability to execute arbitrary commands and gain system privileges. **CVE ID: CVE-2024-40521**	N/A	A-SEA-SEAC-230724/712

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	12-Jul-2024	8.8	There is a remote code execution vulnerability in SeaCMS 12.9. The vulnerability is caused by phomebak.php writing some variable names passed in without filtering them before writing them into the php file. An authenticated attacker can exploit this vulnerability to execute arbitrary commands and obtain system permissions. **CVE ID: CVE-2024-40522**	N/A	A-SEA-SEAC-230724/713
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2024	7.5	SeaCMS v12.9 has an unauthorized SQL injection vulnerability. The vulnerability is caused by the SQL injection through the cid parameter at /js/player/dmplayer/dmku/index.php?ac=edit, which can cause sensitive database information to be leaked. **CVE ID: CVE-2024-39027**	N/A	A-SEA-SEAC-230724/714
Vendor: shopxo					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: shopxo					
Affected Version(s): * Up to (including) 6.1.0					
Server-Side Request Forgery (SSRF)	05-Jul-2024	8.8	A vulnerability was found in ShopXO up to 6.1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file extend/base/Uploader.php. The manipulation of the argument source leads to server-side request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-270367. NOTE: The original disclosure confuses CSRF with SSRF. **CVE ID: CVE-2024-6524**	N/A	A-SHO-SHOP-230724/715
Vendor: Siemens					
Product: medicalis_workflow_orchestrator					
Affected Version(s): *					
N/A	08-Jul-2024	7.8	A vulnerability has been identified in Medicalis Workflow Orchestrator (All versions). The affected application	N/A	A-SIE-MEDI-230724/716

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executes as a trusted account with high privileges and network access. This could allow an authenticated local attacker to escalate privileges. **CVE ID: CVE-2024-37999**		
Vendor: sitetweet_project					
Product: sitetweet					
Affected Version(s): * Up to (including) 0.2					
Cross-Site Request Forgery (CSRF)	02-Jul-2024	8.8	The sitetweet WordPress plugin through 0.2 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-2024-5767**	N/A	A-SIT-SITE-230724/717
Vendor: smashballoon					
Product: feeds_for_youtube					
Affected Version(s): * Up to (excluding) 2.2.2					
Improper Neutralization of Input During Web Page Generation	11-Jul-2024	5.4	The Feeds for YouTube (YouTube video, channel, and gallery plugin) plugin for WordPress is	https://plugins.trac.wordpress.org/changeset/3107577/	A-SMA-FEED-230724/718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerable to Stored Cross-Site Scripting via the plugin's 'youtube-feed' shortcode in all versions up to, and including, 2.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. 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-2024-6256**		
Vendor: space_management_system_project					
Product: space_management_system					
Affected Version(s): * Up to (excluding) 2024-04-09-3302					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Jul-2024	9.8	AguardNet's Space Management System does not properly validate user input, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents. **CVE ID: CVE-2024-6743**	N/A	A-SPA-SPAC-230724/719

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	15-Jul-2024	5.4	AguardNet Technology's Space Management System does not properly filter user input, allowing remote attackers with regular privileges to inject JavaScript and perform Reflected Cross-site scripting attacks. **CVE ID: CVE-2024-6742**	N/A	A-SPA-SPAC-230724/720
Affected Version(s): 2024-04-09-3302					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Jul-2024	9.8	AguardNet's Space Management System does not properly validate user input, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents. **CVE ID: CVE-2024-6743**	N/A	A-SPA-SPAC-230724/721
Vendor: spider-themes					
Product: eazydocs					
Affected Version(s): * Up to (excluding) 2.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-2024	4.8	The EazyDocs WordPress plugin before 2.5.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to	N/A	A-SPI-EAZY-230724/722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID: CVE-2024-3999**		
Vendor: staxwp					
Product: stax					
Affected Version(s): * Up to (including) 1.4.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in StaxWP Elementor Addons, Widgets and Enhancements – Stax allows Stored XSS.This issue affects Elementor Addons, Widgets and Enhancements – Stax: from n/a through 1.4.4.1. **CVE ID: CVE-2024-37541**	N/A	A-STA-STAX-230724/723
Vendor: stitionai					
Product: devika					
Affected Version(s): -					
Improper Neutralization of Input During Web Page	08-Jul-2024	6.1	A stored Cross-Site Scripting (XSS) vulnerability exists in the stitionai/devika	https://github.com/stitionai/devika/commit/6acce21fb08c3d1123ef05df6a3	A-STI-DEVI-230724/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			chat feature, allowing attackers to inject malicious payloads into the chat input. This vulnerability is due to the lack of input validation and sanitization on both the frontend and backend components of the application. Specifically, the application fails to sanitize user input in the chat feature, leading to the execution of arbitrary JavaScript code in the context of the user's browser session. This issue affects all versions of the application. The impact of this vulnerability includes the potential for stolen credentials, extraction of sensitive information from chat logs, projects, and other data accessible through the application. **CVE ID: CVE-2024-5711**	3912bf0ee77c2, https://huntr.com/bounties/6c00ff84-574b-4b4f-bd58-aa7ec1809662	
Vendor: stylemixthemes					
Product: cost_calculator_builder					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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) 3.2.13					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-2024	4.8	The Cost Calculator Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'textarea.description' parameter in all versions up to, and including, 3.2.12 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-6011**	https://plugins.trac.wordpress.org/changeset/3108606/	A-STY-COST-230724/725
Missing Authorization	02-Jul-2024	4.3	The Cost Calculator Builder plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'embed-create-page' and 'embed-insert-pages' functions in all versions up to, and	https://plugins.trac.wordpress.org/changeset/3108606/	A-STY-COST-230724/726

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
			including, 3.2.12. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create arbitrary posts and append arbitrary content to existing posts. **CVE ID: CVE-2024-6012**		
Product: motors_-_car_dealer\,_classifieds_\&_listing					
Affected Version(s): * Up to (excluding) 1.4.11					
Missing Authorization	02-Jul-2024	5.3	The Motors – Car Dealer, Classifieds & Listing plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the stm_edit_delete_user_car function in all versions up to, and including, 1.4.8. This makes it possible for unauthenticated attackers to unpublish arbitrary posts and pages. **CVE ID: CVE-2024-5545**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3106579%40motors-car-dealership-classified-listings%2Ftrunk&old=3101090%40motors-car-dealership-classified-listings%2Ftrunk&sfp_email=&sfph_mail=	A-STY-MOTO-230724/727
Vendor: supsystic					
Product: easy_google_maps					
Affected Version(s): * Up to (excluding) 1.11.16					

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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-2024	5.4	The Easy Google Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file upload feature in all versions up to, and including, 1.11.15 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5219**	https://plugins.trac.wordpress.org/changeset/3105921/	A-SUP-EASY-230724/728
Vendor: syedbalkhi					
Product: wp_lightbox_2					
Affected Version(s): * Up to (excluding) 3.0.6.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jul-2024	5.4	The WP Lightbox 2 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title' parameter in all versions up to, and including, 3.0.6.6 due to insufficient input sanitization and	https://plugins.trac.wordpress.org/changeset?new=3108386%40wp-lightbox-2&old=3046989%40wp-lightbox-2	A-SYE-WP_L-230724/729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2024-6263**		
Vendor: themeruby					
Product: foxiz					
Affected Version(s): * Up to (excluding) 2.3.6					
Server-Side Request Forgery (SSRF)	06-Jul-2024	9.3	Server-Side Request Forgery (SSRF) vulnerability in Theme-Ruby Foxiz.This issue affects Foxiz: from n/a through 2.3.5. **CVE ID: CVE-2024-37260**	N/A	A-THE-FOXI-230724/730
Vendor: thimpress					
Product: learnpress					
Affected Version(s): * Up to (excluding) 4.2.6.8.2					
Missing Authorization	02-Jul-2024	5.3	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to unauthorized user registration due to a missing capability check on the	https://plugins.trac.wordpress.org/changeset/3109339/	A-THI-LEAR-230724/731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'register' function in all versions up to, and including, 4.2.6.8.1. This makes it possible for unauthenticated attackers to bypass disabled user registration to create a new account with the default role. **CVE ID: CVE-2024-6088**		
N/A	02-Jul-2024	5.3	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to unauthenticated bypass to user registration in versions up to, and including, 4.2.6.8.1. This is due to missing checks in the 'check_validate_fields' function in the checkout. This makes it possible for unauthenticated attackers to register as the default role on the site, even if registration is disabled. **CVE ID: CVE-2024-6099**	https://plugins.trac.wordpress.org/changeset/3109339/	A-THI-LEAR-230724/732

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: Tipsandtricks-hq					
Product: wp_estore					
Affected Version(s): * Up to (excluding) 8.5.5					
Cross-Site Request Forgery (CSRF)	15-Jul-2024	8.8	The wp-cart-for-digital-products WordPress plugin before 8.5.5 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks **CVE ID: CVE-2024-6075**	N/A	A-TIP-WP_E-230724/733
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Jul-2024	6.1	The wp-cart-for-digital-products WordPress plugin before 8.5.5 does not escape the $_SERVER['REQUEST_URI'] parameter before outputting it back in an attribute, which could lead to Reflected Cross-Site Scripting in old web browsers **CVE ID: CVE-2024-6072**	N/A	A-TIP-WP_E-230724/734
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Jul-2024	6.1	The wp-cart-for-digital-products WordPress plugin before 8.5.5 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-	N/A	A-TIP-WP_E-230724/735

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Scripting which could be used against high privilege users such as admin **CVE ID: CVE-2024-6073**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Jul-2024	6.1	The wp-cart-for-digital-products WordPress plugin before 8.5.5 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID: CVE-2024-6074**	N/A	A-TIP-WP_E-230724/736
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Jul-2024	6.1	The wp-cart-for-digital-products WordPress plugin before 8.5.5 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID: CVE-2024-6076**	N/A	A-TIP-WP_E-230724/737
Vendor: unlimited-elements					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: unlimited_elements_for_elementor_\(free_widgets\,_addons\,_templates\)					
Affected Version(s): * Up to (excluding) 1.5.113					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Jul-2024	8.8	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to time-based SQL Injection via the 'addons_order' parameter in all versions up to, and including, 1.5.112 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above and granted plugin setting edit permissions by an administrator, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2024-6166**	https://plugins.trac.wordpress.org/browser/unlimited-elements-for-elementor/trunk/inc_php/unitecreator_addons.class.php#L79, https://plugins.trac.wordpress.org/changeset/3112307/	A-UNL-UNLI-230724/738

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	09-Jul-2024	5.4	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'username' parameter in all versions up to, and including, 1.5.112 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above and granted plugin setting edit permissions by an administrator, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-6169**	https://plugins.trac.wordpress.org/browser/unlimited-elements-for-elementor/trunk/inc_php/framework/instagram/helper.class.php#L168, https://plugins.trac.wordpress.org/changeset/3112307/	A-UNL-UNLI-230724/739
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	5.4	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the	https://plugins.trac.wordpress.org/browser/unlimited-elements-for-elementor/trunk/inc_php/unitecreator_settings_output.class.p	A-UNL-UNLI-230724/740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'email' parameter in all versions up to, and including, 1.5.112 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-2024-6170**	hp#L398, https://plugins.trac.wordpress.org/changeset/3112307/	
N/A	09-Jul-2024	5.3	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to IP Address Spoofing in all versions up to, and including, 1.5.112 due to insufficient IP address validation and/or use of user-supplied HTTP headers as a primary method for IP retrieval. This makes it possible for unauthenticated attackers to bypass	https://plugins.trac.wordpress.org/browser/unlimited-elements-for-elementor/trunk/inc_php/framework/functions.class.php#L3407, https://plugins.trac.wordpress.org/browser/unlimited-elements-for-elementor/trunk/inc_php/unitecreator_form.class.php#L742	A-UNL-UNLI-230724/741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			antispam functionality in the Form Builder widgets. **CVE ID: CVE-2024-6171**		
Vendor: vaethink					
Product: vaethink					
Affected Version(s): 1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-2024	5.4	vaeThink 1.0.2 is vulnerable to stored Cross Site Scripting (XSS) in the system backend. **CVE ID: CVE-2024-38971**	N/A	A-VAE-VAET-230724/742
N/A	09-Jul-2024	4.9	vaeThink 1.0.2 is vulnerable to Information Disclosure via the system backend,access management administrator function. **CVE ID: CVE-2024-38970**	N/A	A-VAE-VAET-230724/743
Vendor: Vmware					
Product: aria_automation					
Affected Version(s): * Up to (excluding) 8.17.0					
Improper Neutralization of Special Elements used in an SQL Command	11-Jul-2024	8.1	VMware Aria Automation does not apply correct input validation which allows for SQL-injection in the product. An authenticated malicious user	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24598	A-VMW-ARIA-230724/744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			could enter specially crafted SQL queries and perform unauthorised read/write operations in the database. **CVE ID: CVE-2024-22280**		
Product: cloud_foundation					
Affected Version(s): From (including) 4.0 Up to (including) 5.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Jul-2024	8.1	VMware Aria Automation does not apply correct input validation which allows for SQL-injection in the product. An authenticated malicious user could enter specially crafted SQL queries and perform unauthorised read/write operations in the database. **CVE ID: CVE-2024-22280**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24598	A-VMW-CLOU-230724/745
Vendor: voidcoders					
Product: void_contact_form_7_widget_for_elementor_page_builder					
Affected Version(s): * Up to (excluding) 2.4.1					
Improper Neutralization of Input During Web Page Generation	02-Jul-2024	5.4	The Void Contact Form 7 Widget For Elementor Page Builder plugin for WordPress is vulnerable to Stored Cross-Site	https://plugins.trac.wordpress.org/changeset/3109802/#file6	A-VOI-VOID-230724/746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Scripting via the 'cf7_redirect_page' attribute within the plugin's Void Contact From 7 widget in all versions up to, and including, 2.4 due to insufficient input sanitization and output escaping on user supplied attributes. 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-2024-5419**		
Vendor: wbolt					
Product: imgspider					
Affected Version(s): * Up to (excluding) 2.3.11					
Unrestricted Upload of File with Dangerous Type	04-Jul-2024	8.8	The IMGspider plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'upload_img_file' function in all versions up to, and including, 2.3.10. This makes it	https://plugins.trac.wordpress.org/changeset/3107741/imgspider	A-WBO-IMGS-230724/747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible for authenticated attackers, with contributor-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible. **CVE ID: CVE-2024-6318**		
Unrestricted Upload of File with Dangerous Type	04-Jul-2024	8.8	The IMGspider plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'upload' function in all versions up to, and including, 2.3.10. This makes it possible for authenticated attackers, with contributor-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible. **CVE ID: CVE-2024-6319**	https://plugins.trac.wordpress.org/changeset/3107741/imgspider	A-WBO-IMGS-230724/748
Vendor: webnus					
Product: modern_events_calendar					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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) 7.12.0					
Unrestricted Upload of File with Dangerous Type	09-Jul-2024	8.8	The Modern Events Calendar plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the set_featured_image function in all versions up to, and including, 7.11.0. This makes it possible for authenticated attackers, with subscriber access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. The plugin allows administrators (via its settings) to extend the ability to submit events to unauthenticated users, which would allow unauthenticated attackers to exploit this vulnerability. **CVE ID: CVE-2024-5441**	N/A	A-WEB-MODE-230724/749
Product: modern_events_calendar_lite					
Affected Version(s): * Up to (including) 6.5.6					
Unrestricted Upload of	09-Jul-2024	8.8	The Modern Events Calendar plugin for	N/A	A-WEB-MODE-230724/750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the set_featured_image function in all versions up to, and including, 7.11.0. This makes it possible for authenticated attackers, with subscriber access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. The plugin allows administrators (via its settings) to extend the ability to submit events to unauthenticated users, which would allow unauthenticated attackers to exploit this vulnerability. **CVE ID: CVE-2024-5441**		
Vendor: wedevs					
Product: wp_erp					
Affected Version(s): * Up to (excluding) 1.13.1					
Improper Neutralization of Special	11-Jul-2024	8.8	The WP ERP plugin for WordPress is vulnerable to SQL Injection via the	https://plugins.trac.wordpress.org/changeset/3064874/erp/t	A-WED-WP_E-230724/751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			'vendor_id' parameter in all versions up to, and including, 1.13.0 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 Accounting Manager access (erp_ac_view_sales_summary capability) and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2024-6666**	ags/1.13.1/modules/accounting/includes/functions/transactions.php	
Vendor: wisdomgarden					
Product: tronclass					
Affected Version(s): * Up to (excluding) 1.69.61976					
N/A	15-Jul-2024	5.3	The tumbnail API of Tronclass from WisdomGarden lacks proper access control, allowing unauthenticated remote attackers to obtain certain	N/A	A-WIS-TRON-230724/752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific files by modifying the URL. **CVE ID: CVE-2024-6738**		
Vendor: wpexpertplugins					
Product: post_meta_data_manager					
Affected Version(s): * Up to (excluding) 1.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-2024	5.4	The Post Meta Data Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '$meta_key' parameter in all versions up to, and including, 1.2.3 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-2024-6264**	https://plugins.trac.wordpress.org/changeset/3109558/	A-WPE-POST-230724/753
Vendor: wpmudev					
Product: branda					
Affected Version(s): * Up to (excluding) 3.4.19					
N/A	11-Jul-2024	5.3	The Branda – White Label WordPress, Custom Login Page	https://plugins.trac.wordpress.org/changeset?	A-WPM-BRAN-230724/754

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
			Customizer plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 3.4.18. This is due the plugin utilizing composer without preventing direct access to the files. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website. **CVE ID: CVE-2024-6554**	sfp_email=&sfph_mail=&reponame=&old=3115603%40branda-white-labeling&new=3115603%40branda-white-labeling&sfp_email=&sfph_mail=	
Vendor: wpserveur					
Product: wps_hide_login					
Affected Version(s): * Up to (excluding) 1.9.16.4					
URL Redirection to Untrusted Site ('Open Redirect')	15-Jul-2024	6.1	The WPS Hide Login WordPress plugin before 1.9.16.4 does not prevent redirects to the login page via the auth_redirect WordPress	N/A	A-WPS-WPS_-230724/755

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
			function, allowing an unauthenticated visitor to access the hidden login page. **CVE ID: CVE-2024-6289**		
Vendor: yeken					
Product: snippet_shortcodes					
Affected Version(s): * Up to (excluding) 4.1.5					
Cross-Site Request Forgery (CSRF)	03-Jul-2024	4.3	The Snippet Shortcodes plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.1.4. This is due to missing or incorrect nonce validation when adding or editing shortcodes. This makes it possible for unauthenticated attackers to modify shortcodes via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-4543**	https://plugins.trac.wordpress.org/changeset/3110951?contextall=1	A-YEK-SNIP-230724/756
Vendor: zblogcn					
Product: z-blogphp					
Affected Version(s): * Up to (including) 1.7.3.3230					

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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-2024	6.1	A cross-site scripting (XSS) vulnerability in the Backend Theme Management module of Z-BlogPHP v1.7.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload. **CVE ID: CVE-2024-39203**	N/A	A-ZBL-Z-BL-230724/757
Vendor: zealousweb					
Product: generate_pdf_using_contact_form_7					
Affected Version(s): * Up to (including) 4.0.9					
Unrestricted Upload of File with Dangerous Type	09-Jul-2024	9.8	Unrestricted Upload of File with Dangerous Type vulnerability in ZealousWeb Generate PDF using Contact Form 7.This issue affects Generate PDF using Contact Form 7: from n/a through 4.0.6. **CVE ID: CVE-2024-37555**	N/A	A-ZEA-GENE-230724/758
Vendor: zkteco					
Product: biotime					
Affected Version(s): From (including) 8.5 Up to (including) 9.5.2					
Improper Neutralization of Input During Web Page Generation	05-Jul-2024	5.4	A vulnerability was found in ZKTeco BioTime up to 9.5.2. It has been classified as problematic.	N/A	A-ZKT-BIOT-230724/759

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')			Affected is an unknown function of the component system-group-add Handler. The manipulation of the argument user with the input <script>alert('XSS')</script> leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-270366 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-6523**		
Hardware					
Vendor: ABB					
Product: aspect-ent-12					
Affected Version(s): -					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga	H-ABB-ASPE-230724/760

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01; MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**	=2.39956449.23035250.1719878527-141379670.1701144964	
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-ASPE-230724/761
Product: aspect-ent-2					
Affected Version(s): -					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.2	H-ABB-ASPE-230724/762

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01; MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**	3035250.1719878527-141379670.1701144964	
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-ASPE-230724/763
Product: aspect-ent-256					
Affected Version(s): -					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.17198	H-ABB-ASPE-230724/764

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01; MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**	78527-141379670.1701144964	
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-ASPE-230724/765
Product: aspect-ent-96					
Affected Version(s): -					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-	H-ABB-ASPE-230724/766

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise: through 3.08.01; NEXUS Series: through 3.08.01; MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**	141379670.1701144964	
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-ASPE-230724/767
Product: matrix-11					
Affected Version(s): -					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise:	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-	H-ABB-MATR-230724/768

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 3.08.01; NEXUS Series: through 3.08.01; MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**	141379670.1701144964	
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-MATR-230724/769
Product: matrix-216					
Affected Version(s): -					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-MATR-230724/770

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NEXUS Series: through 3.08.01; MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-MATR-230724/771
Product: matrix-232					
Affected Version(s): -					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series:	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-MATR-230724/772

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 3.08.01; MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-MATR-230724/773
Product: matrix-264					
Affected Version(s): -					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-MATR-230724/774

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-MATR-230724/775
Product: matrix-296					
Affected Version(s): -					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-MATR-230724/776

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-MATR-230724/777
Product: nexus-2128					
Affected Version(s): -					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/778

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/779
Product: nexus-2128-a					
Affected Version(s): -					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/780

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/781
Product: nexus-2128-f					
Affected Version(s): -					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/782

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/783
Product: nexus-2128-g					
Affected Version(s): -					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/785
Product: nexus-264					
Affected Version(s): -					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/786

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/787
Product: nexus-264-a					
Affected Version(s): -					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/788

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/789
Product: nexus-264-f					
Affected Version(s): -					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/791
Product: nexus-264-g					
Affected Version(s): -					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/793
Product: nexus-3-2128					
Affected Version(s): -					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/794

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/795
Product: nexus-3-264					
Affected Version(s): -					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/796

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	H-ABB-NEXU-230724/797
Vendor: Cisco					
Product: mds_9000					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/798

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9100					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-MDS_-230724/799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials.	nxos-cmd-injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-20399		
Product: mds_9132t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9134					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/801

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9140					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9148					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9148s					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/804

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9148t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9200					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9216					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9216a					
Affected Version(s): -					
Improper Neutralization of	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could	https://sec.cloudapps.cisco.com/security/cente	H-CIS-MDS_-230724/808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	r/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9216i					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9222i					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9250i					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9396s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-	H-CIS-MDS_-230724/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**	injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: mds_9396t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/813

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9500					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9506					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9509					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/816

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9513					
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')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/817

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9700					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9706					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9710					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-MDS_-230724/820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: mds_9718					
Affected Version(s): -					
Improper Neutralization of Special Elements	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-MDS_-230724/821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials.	y/cisco-sa-nxos-cmd-injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-20399		
Product: nexus_3000					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3016					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/823

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
			successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3016q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3048					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_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
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/826

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
			this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3064-32t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/827

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3064-t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/828

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3064-x					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3064t					
Affected Version(s): -					
Improper Neutralization of	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could	https://sec.cloudapps.cisco.com/security/cente	H-CIS-NEXU-230724/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	r/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3064x					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3100					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3100-v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3100-z					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-	H-CIS-NEXU-230724/834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**	injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: nexus_3100v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/835

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_31108pc-v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_31108pv-v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_31108tc-v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/838

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_31128pq					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3132c-z					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3132q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3132q-v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3132q-x					
Affected Version(s): -					
Improper Neutralization of Special Elements	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-NEXU-230724/843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials.	y/cisco-sa-nxos-cmd-injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-20399		
Product: nexus_3132q-xl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3132q-x\/3132q-xl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3164q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3172					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3172pq					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/848

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3172pq-xl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/849

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3172pq\/pq-xl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/850

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3172tq					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3172tq-32t					
Affected Version(s): -					
Improper Neutralization of	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could	https://sec.cloudapps.cisco.com/security/cente	H-CIS-NEXU-230724/852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	r/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3172tq-xl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3200					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3232					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3232c					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-	H-CIS-NEXU-230724/856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**	injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: nexus_3232c_					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/857

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3264c-e					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3264q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3400					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/860

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3408-s					
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')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_34180yc					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_34200yc-sm					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3432d-s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3464c					
Affected Version(s): -					
Improper Neutralization of Special Elements	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-NEXU-230724/865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials.	y/cisco-sa-nxos-cmd-injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-20399		
Product: nexus_3500					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3524					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/867

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3524-x					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3524-xl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3524-x\/xl					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/870

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3548					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3548-x					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3548-xl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/873

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3548-x\/xl					
Affected Version(s): -					
Improper Neutralization of	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could	https://sec.cloudapps.cisco.com/security/cente	H-CIS-NEXU-230724/874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	r/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3600					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_36180yc-r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_3636c-r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_5000					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-	H-CIS-NEXU-230724/878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**	injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: nexus_5010					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/879

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_5020					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/880

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
			could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_5500					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_5548p					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/882

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_5548up					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/883

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_5596t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_5596up					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_5600					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_56128p					
Affected Version(s): -					
Improper Neutralization of Special Elements	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-NEXU-230724/887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials.	y/cisco-sa-nxos-cmd-injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-20399		
Product: nexus_5624q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_5648q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/889

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_5672up					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_5672up-16g					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_5696q					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/892

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7000					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7000_10-slot					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7000_18-slot					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/895

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7000_4-slot					
Affected Version(s): -					
Improper Neutralization of	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could	https://sec.cloudapps.cisco.com/security/cente	H-CIS-NEXU-230724/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	r/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7000_9-slot					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7000_supervisor_1					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/898

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
			affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7000_supervisor_2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7000_supervisor_2e					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-	H-CIS-NEXU-230724/900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**	injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: nexus_7004					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/901

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7009					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7010					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7018					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/904

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7700					
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')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/905

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7700_10-slot					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7700_18-slot					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7700_2-slot					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7700_6-slot					
Affected Version(s): -					
Improper Neutralization of Special Elements	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-NEXU-230724/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials.	y/cisco-sa-nxos-cmd-injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-20399		
Product: nexus_7700_supervisor_2e					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/910

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7700_supervisor_3e					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7702					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7706					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7710					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_7718					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9000					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9000v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9000_in_aci_mode					
Affected Version(s): -					
Improper Neutralization of	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could	https://sec.cloudapps.cisco.com/security/cente	H-CIS-NEXU-230724/918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	r/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9000_in_standalone					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9000_in_standalone_nx-os_mode					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9200					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9200yc					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-	H-CIS-NEXU-230724/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**	injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: nexus_92160yc-x					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/923

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9221c					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/924

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_92300yc					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_92304qc					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/926

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9232e					
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')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/927

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_92348gc-x					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9236c					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9272q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9300					
Affected Version(s): -					
Improper Neutralization of Special Elements	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-NEXU-230724/931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials.	y/cisco-sa-nxos-cmd-injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-20399		
Product: nexus_93108tc-ex					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/932

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93108tc-ex-24					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/933

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93108tc-fx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93108tc-fx-24					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93108tc-fx3h					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/936

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93108tc-fx3p					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/937

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93120tx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/938

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93128					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93128tx					
Affected Version(s): -					
Improper Neutralization of	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could	https://sec.cloudapps.cisco.com/security/cente	H-CIS-NEXU-230724/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	r/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9316d-gx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93180lc-ex					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93180tc-ex					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93180yc-ex					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-	H-CIS-NEXU-230724/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**	injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: nexus_93180yc-ex-24					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/945

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93180yc-fx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93180yc-fx-24					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93180yc-fx3					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/948

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93180yc-fx3h					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/949

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
			device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93180yc-fx3s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93216tc-fx2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93240tc-fx2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93240yc-fx2					
Affected Version(s): -					
Improper Neutralization of Special Elements	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-NEXU-230724/953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials.	y/cisco-sa-nxos-cmd-injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-20399		
Product: nexus_9332c					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9332d-gx2b					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/955

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9332d-h2r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9332pq					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_93360yc-fx2					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/958

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
			this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9336c-fx2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/959

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9336c-fx2-e					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9336pq					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/961

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9336pq_aci					
Affected Version(s): -					
Improper Neutralization of	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could	https://sec.cloudapps.cisco.com/security/cente	H-CIS-NEXU-230724/962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	r/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9336pq_aci_spine					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9348d-gx2a					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9348gc-fx3					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9348gc-fxp					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-	H-CIS-NEXU-230724/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**	injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: nexus_93600cd-gx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/967

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9364c					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/968

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
			could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9364c-gx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9364d-gx2a					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/970

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9372px					
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')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/971

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9372px-e					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9372tx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9372tx-e					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9396px					
Affected Version(s): -					
Improper Neutralization of Special Elements	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-NEXU-230724/975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials.	y/cisco-sa-nxos-cmd-injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-20399		
Product: nexus_9396tx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9408					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/977

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9432pq					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9500					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9500r					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/980

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
			this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9500_16-slot					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/981

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
			arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9500_4-slot					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9500_8-slot					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/983

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9500_supervisor_a					
Affected Version(s): -					
Improper Neutralization of	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could	https://sec.cloudapps.cisco.com/security/cente	H-CIS-NEXU-230724/984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	r/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9500_supervisor_a\+					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9500_supervisor_b					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9500_supervisor_b\+					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9504					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-	H-CIS-NEXU-230724/988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**	injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: nexus_9508					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/989

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9516					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/990

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9536pq					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9636pq					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/992

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9716d-gx					
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')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9736pq					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9800					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9804					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	H-CIS-NEXU-230724/996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Product: nexus_9808					
Affected Version(s): -					
Improper Neutralization of Special Elements	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-NEXU-230724/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials.	y/cisco-sa-nxos-cmd-injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-20399		
Vendor: Dlink					
Product: dar-7000					
Affected Version(s): -					
Deserialization of Untrusted Data	05-Jul-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DAR-7000 up to 20230922. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /log/decodmail.php. The manipulation of the argument file leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-270368. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID: CVE-2024-6525**	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10354	H-DLI-DAR--230724/998
Product: dir-823x_ax3000					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
N/A	08-Jul-2024	8.8	D-Link DIR-823X firmware - 240126 was discovered to contain a remote command execution (RCE) vulnerability via the dhcpd_startip parameter at /goform/set_lan_settings. **CVE ID: CVE-2024-39202**	N/A	H-DLI-DIR--230724/999
Vendor: kiloview					
Product: p1					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-2024	5.4	A 'Cross-site Scripting' (XSS) vulnerability, characterized by improper input neutralization during web page generation, has been discovered. This vulnerability allows for Stored XSS attacks to occur. Multiple areas within the administration interface of the webserver lack adequate input validation, resulting in multiple instances of Stored XSS vulnerabilities.	N/A	H-KIL-P1-230724/1000

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2023-41922		
Product: p2					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-2024	5.4	A 'Cross-site Scripting' (XSS) vulnerability, characterized by improper input neutralization during web page generation, has been discovered. This vulnerability allows for Stored XSS attacks to occur. Multiple areas within the administration interface of the webserver lack adequate input validation, resulting in multiple instances of Stored XSS vulnerabilities. **CVE ID: CVE-2023-41922**	N/A	H-KIL-P2-230724/1001
Vendor: level1					
Product: wbr-6013					
Affected Version(s): -					
Use of Hard-coded Credentials	08-Jul-2024	9.8	A hard-coded password vulnerability exists in the telnetd functionality of LevelOne WBR-6013 RER4_A_v3411b_2T2R_LEV_09_1706	N/A	H-LEV-WBR--230724/1002

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			23. A set of specially crafted network packets can lead to arbitrary command execution. **CVE ID: CVE-2023-46685**		
Cross-Site Request Forgery (CSRF)	08-Jul-2024	8.8	A cross-site request forgery (csrf) vulnerability exists in the boa CSRF protection functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted network request can lead to CSRF. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID: CVE-2023-47677**	N/A	H-LEV-WBR--230724/1003
Improper Verification of Cryptographic Signature	08-Jul-2024	7.2	A firmware update vulnerability exists in the boa formUpload functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted network packets can lead to arbitrary firmware update. An attacker can provide a malicious file to trigger this vulnerability.	N/A	H-LEV-WBR--230724/1004

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2023-34435		
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa formRoute functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID: CVE-2023-41251**	N/A	H-LEV-WBR--230724/1005
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa setRepeaterSsid functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID: CVE-2023-45215**	N/A	H-LEV-WBR--230724/1006
Integer Overflow	08-Jul-2024	7.2	An integer overflow vulnerability exists	N/A	H-LEV-WBR--230724/1007

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Wraparound			in the boa updateConfigIntoFlash functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID: CVE-2023-45742**		
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa set_RadvdPrefixParam functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID: CVE-2023-47856**	N/A	H-LEV-WBR--230724/1008
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa formDnsv6 functionality of Realtek rtl819x Jungle SDK v3.4.11.	N/A	H-LEV-WBR--230724/1009

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 specially crafted series of network requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID: CVE-2023-48270**		
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa formFilter functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID: CVE-2023-49073**	N/A	H-LEV-WBR--230724/1010
N/A	08-Jul-2024	7.2	Leftover debug code exists in the boa formSysCmd functionality of LevelOne WBR-6013 RER4_A_v3411b_2T2R_LEV_09_170623. A specially crafted network request can lead to	N/A	H-LEV-WBR--230724/1011

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 command execution. **CVE ID: CVE-2023-49593**		
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa rollback_control_code functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID: CVE-2023-49595**	N/A	H-LEV-WBR--230724/1012
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send a series of HTTP requests to trigger this vulnerability. **CVE ID: CVE-2023-49867**	N/A	H-LEV-WBR--230724/1013

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	08-Jul-2024	7.2	Two stack-based buffer overflow vulnerabilities exist in the boa set_RadvdInterface Param functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `interfacename` request's parameter. **CVE ID: CVE-2023-50239**	N/A	H-LEV-WBR--230724/1014
Out-of-bounds Write	08-Jul-2024	7.2	Two stack-based buffer overflow vulnerabilities exist in the boa set_RadvdInterface Param functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to remote code execution. An attacker can send a sequence of	N/A	H-LEV-WBR--230724/1015

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `AdvDefaultPreference` request's parameter. **CVE ID: CVE-2023-50240**		
Out-of-bounds Write	08-Jul-2024	7.2	Two stack-based buffer overflow vulnerabilities exist in the boa formIpQoS functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `comment` request's parameter. **CVE ID: CVE-2023-50243**	N/A	H-LEV-WBR--230724/1016
Out-of-bounds Write	08-Jul-2024	7.2	Two stack-based buffer overflow vulnerabilities exist in the boa formIpQoS functionality of Realtek rtl819x	N/A	H-LEV-WBR--230724/1017

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `entry_name` request's parameter. **CVE ID: CVE-2023-50244**		
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa getInfo functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send a series of HTTP requests to trigger this vulnerability. **CVE ID: CVE-2023-50330**	N/A	H-LEV-WBR--230724/1018
Improper Neutralization of Special Elements used in an OS	08-Jul-2024	7.2	Three os command injection vulnerabilities exist in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11.	N/A	H-LEV-WBR--230724/1019

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 ('OS Command Injection')			A specially crafted series of HTTP requests can lead to arbitrary command execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This command injection is related to the `targetAPSsid` request's parameter. **CVE ID: CVE-2023-50381**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jul-2024	7.2	Three os command injection vulnerabilities exist in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary command execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This command injection is related to the `peerPin` request's parameter. **CVE ID: CVE-2023-50382**	N/A	H-LEV-WBR--230724/1020
Improper Neutralization of	08-Jul-2024	7.2	Three os command injection vulnerabilities exist	N/A	H-LEV-WBR--230724/1021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary command execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This command injection is related to the `localPin` request's parameter. **CVE ID: CVE-2023-50383**		
Out-of-bounds Write	08-Jul-2024	7.2	A heap-based buffer overflow vulnerability exists in the configuration file mib_init_value_array functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted .dat file can lead to arbitrary code execution. An attacker can upload a malicious file to trigger this vulnerability. **CVE ID: CVE-2024-21778**	N/A	H-LEV-WBR--230724/1022
Vendor: Mitsubishielectric					
Product: mrzjw3-mc2-utl					
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
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	H-MIT-MRZJ-230724/1023
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	H-MIT-MRZJ-230724/1024
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	H-MIT-MRZJ-230724/1025
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges	N/A	H-MIT-MRZJ-230724/1026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and execute arbitrary code. **CVE ID: CVE-2024-25088**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	H-MIT-MRZJ-230724/1027
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	H-MIT-MRZJ-230724/1028
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	H-MIT-MRZJ-230724/1029
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0	N/A	H-MIT-MRZJ-230724/1030

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 cause a Windows blue screen error. **CVE ID: CVE-2024-22102**		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	H-MIT-MRZJ-230724/1031
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	H-MIT-MRZJ-230724/1032
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	H-MIT-MRZJ-230724/1033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	H-MIT-MRZJ-230724/1034
Product: sw0dnc-mneth-b					
Affected Version(s): -					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	H-MIT-SW0D-230724/1035
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	H-MIT-SW0D-230724/1036
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local	N/A	H-MIT-SW0D-230724/1037

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	H-MIT-SW0D-230724/1038
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	H-MIT-SW0D-230724/1039
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	H-MIT-SW0D-230724/1040
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver	N/A	H-MIT-SW0D-230724/1041

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	H-MIT-SW0D-230724/1042
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	H-MIT-SW0D-230724/1043
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	N/A	H-MIT-SW0D-230724/1044

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-22104		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	H-MIT-SW0D-230724/1045
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	H-MIT-SW0D-230724/1046
Product: sw1dnc-ccbd2-b					
Affected Version(s): -					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	H-MIT-SW1D-230724/1047
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to	N/A	H-MIT-SW1D-230724/1048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	H-MIT-SW1D-230724/1049
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	H-MIT-SW1D-230724/1050
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	H-MIT-SW1D-230724/1051

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
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	H-MIT-SW1D-230724/1052
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	H-MIT-SW1D-230724/1053
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	H-MIT-SW1D-230724/1054
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	N/A	H-MIT-SW1D-230724/1055

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-22103		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	H-MIT-SW1D-230724/1056
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	H-MIT-SW1D-230724/1057
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	H-MIT-SW1D-230724/1058
Product: sw1dnc-ccief-b					
Affected Version(s): -					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local	N/A	H-MIT-SW1D-230724/1059

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	H-MIT-SW1D-230724/1060
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	H-MIT-SW1D-230724/1061
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	H-MIT-SW1D-230724/1062

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	H-MIT-SW1D-230724/1063
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	H-MIT-SW1D-230724/1064
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	H-MIT-SW1D-230724/1065
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error.	N/A	H-MIT-SW1D-230724/1066

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-22102		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	H-MIT-SW1D-230724/1067
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	H-MIT-SW1D-230724/1068
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	H-MIT-SW1D-230724/1069
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a	N/A	H-MIT-SW1D-230724/1070

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
			Windows blue screen error. **CVE ID: CVE-2024-25087**		
Product: sw1dnc-ccief-j					
Affected Version(s): -					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	H-MIT-SW1D-230724/1071
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	H-MIT-SW1D-230724/1072
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	H-MIT-SW1D-230724/1073

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	H-MIT-SW1D-230724/1074
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	H-MIT-SW1D-230724/1075
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	H-MIT-SW1D-230724/1076
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	N/A	H-MIT-SW1D-230724/1077

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2023-51778		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	H-MIT-SW1D-230724/1078
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	H-MIT-SW1D-230724/1079
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	H-MIT-SW1D-230724/1080
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a	N/A	H-MIT-SW1D-230724/1081

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Windows blue screen error. **CVE ID: CVE-2024-22105**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	H-MIT-SW1D-230724/1082
Product: sw1dnc-mnetg-b					
Affected Version(s): -					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	H-MIT-SW1D-230724/1083
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	H-MIT-SW1D-230724/1084

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
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	H-MIT-SW1D-230724/1085
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	H-MIT-SW1D-230724/1086
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	H-MIT-SW1D-230724/1087
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error.	N/A	H-MIT-SW1D-230724/1088

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2023-51777		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	H-MIT-SW1D-230724/1089
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	H-MIT-SW1D-230724/1090
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	H-MIT-SW1D-230724/1091
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a	N/A	H-MIT-SW1D-230724/1092

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	H-MIT-SW1D-230724/1093
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	H-MIT-SW1D-230724/1094
Product: sw1dnc-qsccf-b					
Affected Version(s): -					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	H-MIT-SW1D-230724/1095

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	H-MIT-SW1D-230724/1096
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	H-MIT-SW1D-230724/1097
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	H-MIT-SW1D-230724/1098
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges	N/A	H-MIT-SW1D-230724/1099

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 execute arbitrary code. **CVE ID: CVE-2024-26314**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	H-MIT-SW1D-230724/1100
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	H-MIT-SW1D-230724/1101
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	H-MIT-SW1D-230724/1102
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local	N/A	H-MIT-SW1D-230724/1103

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	H-MIT-SW1D-230724/1104
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	H-MIT-SW1D-230724/1105
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	H-MIT-SW1D-230724/1106
Product: sw1dnd-emsdk-b					
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
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	H-MIT-SW1D-230724/1107
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	H-MIT-SW1D-230724/1108
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	H-MIT-SW1D-230724/1109
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges	N/A	H-MIT-SW1D-230724/1110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and execute arbitrary code. **CVE ID: CVE-2024-25088**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	H-MIT-SW1D-230724/1111
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	H-MIT-SW1D-230724/1112
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	H-MIT-SW1D-230724/1113
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0	N/A	H-MIT-SW1D-230724/1114

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 cause a Windows blue screen error. **CVE ID: CVE-2024-22102**		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	H-MIT-SW1D-230724/1115
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	H-MIT-SW1D-230724/1116
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	H-MIT-SW1D-230724/1117

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	H-MIT-SW1D-230724/1118
Vendor: nuvoton					
Product: npcm705r					
Affected Version(s): -					
Improper Authentication	11-Jul-2024	6.7	Nuvoton - CWE-305: Authentication Bypass by Primary Weakness An attacker with write access to the SPI-Flash on an NPCM7xx BMC subsystem that uses the Nuvoton BootBlock reference code can modify the u-boot image header on flash parsed by the BootBlock which could lead to arbitrary code execution. **CVE ID: CVE-2024-38433**	N/A	H-NUV-NPCM-230724/1119
Product: npcm710r					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	11-Jul-2024	6.7	Nuvoton - CWE-305: Authentication Bypass by Primary Weakness An attacker with write access to the SPI-Flash on an NPCM7xx BMC subsystem that uses the Nuvoton BootBlock reference code can modify the u-boot image header on flash parsed by the BootBlock which could lead to arbitrary code execution. **CVE ID: CVE-2024-38433**	N/A	H-NUV-NPCM-230724/1120
Product: npcm730r					
Affected Version(s): -					
Improper Authentication	11-Jul-2024	6.7	Nuvoton - CWE-305: Authentication Bypass by Primary Weakness An attacker with write access to the SPI-Flash on an NPCM7xx BMC subsystem that	N/A	H-NUV-NPCM-230724/1121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uses the Nuvoton BootBlock reference code can modify the u-boot image header on flash parsed by the BootBlock which could lead to arbitrary code execution. **CVE ID: CVE-2024-38433**		
Product: npcm750r					
Affected Version(s): -					
Improper Authentication	11-Jul-2024	6.7	Nuvoton - CWE-305: Authentication Bypass by Primary Weakness An attacker with write access to the SPI-Flash on an NPCM7xx BMC subsystem that uses the Nuvoton BootBlock reference code can modify the u-boot image header on flash parsed by the BootBlock which could lead to arbitrary code execution.	N/A	H-NUV-NPCM-230724/1122

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-2024-38433		
Vendor: Qualcomm					
Product: 205_mobile_platform					
Affected Version(s): -					
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-205_-230724/1123
Product: 215_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-215_-230724/1124
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-215_-230724/1125
Product: 315_5g_iot_modem					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-315_-230724/1126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21461	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-315_-230724/1127
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-315_-230724/1128
Product: 9205_lte_modem					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-9205-230724/1129
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-9205-230724/1130
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-9205-230724/1131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-9205-230724/1132
Product: apq5053-aa					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-APQ5-230724/1133
Product: apq8017					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-APQ8-230724/1134
Product: apq8037					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-APQ8-230724/1135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: apq8053-aa					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-APQ8-230724/1136
Product: apq8053-ac					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-APQ8-230724/1137
Product: apq8064au					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-APQ8-230724/1138
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-APQ8-230724/1139

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: aqt1000					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AQT1-230724/1140
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AQT1-230724/1141
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AQT1-230724/1142
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AQT1-230724/1143
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AQT1-230724/1144

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AQT1-230724/1145
Product: ar8031					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AR80-230724/1146
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AR80-230724/1147
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AR80-230724/1148
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AR80-230724/1149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AR80-230724/1150
Product: ar8035					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AR80-230724/1151
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AR80-230724/1152
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AR80-230724/1153
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AR80-230724/1154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AR80-230724/1155
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AR80-230724/1156
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AR80-230724/1157
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AR80-230724/1158
Product: ar9380					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-AR93-230724/1159
Product: c-v2x_9150					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-C-V2-230724/1160
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-C-V2-230724/1161
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-C-V2-230724/1162
Product: csr8811					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-CSR8-230724/1163
Buffer Copy without	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicres	H-QUA-CSR8-230724/1164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-CSR8-230724/1165
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-CSR8-230724/1166
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-CSR8-230724/1167
Product: csra6620					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-CSRA-230724/1168
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-CSRA-230724/1169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	bulletin/july-2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-CSRA-230724/1170
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-CSRA-230724/1171
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-CSRA-230724/1172
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-CSRA-230724/1173
Product: csra6640					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-CSRA-230724/1174

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 is freed by keymaster. **CVE ID: CVE-2024-21461**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-CSRA-230724/1175
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-CSRA-230724/1176
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-CSRA-230724/1177
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-CSRA-230724/1178
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-CSRA-230724/1179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: csrb31024					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-CSRB-230724/1180
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-CSRB-230724/1181
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-CSRB-230724/1182
Product: fastconnect_6200					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1183

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1184
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1185
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1186
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1187
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1189
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1190
Product: fastconnect_6700					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1191
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1192
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1193
Buffer Copy without	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicres	H-QUA-FAST-230724/1194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	ources/security bulletin/july-2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1195
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1196
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1197
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1198
Product: fastconnect_6800					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1199
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1200
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1201
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1202
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1203

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1204
Product: fastconnect_6900					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1205
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1206
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1207
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1209
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1210
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1211
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1212
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1213
Product: fastconnect_7800					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1214
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1215
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1216
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1217
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1218

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1219
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1220
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1221
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1222
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1223
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-FAST-230724/1224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			one chunk in virtual address space. **CVE ID: CVE-2024-21460**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FAST-230724/1225
Product: flight_rb5_5g_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FLIG-230724/1226
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FLIG-230724/1227
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FLIG-230724/1228
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-FLIG-230724/1229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FLIG-230724/1230
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FLIG-230724/1231
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FLIG-230724/1232
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FLIG-230724/1233
Product: fsm10055					
Affected Version(s): -					
Buffer Copy without Checking	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicresources/security	H-QUA-FSM1-230724/1234

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	bulletin/july-2024-bulletin.html	
Product: fsm10056					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FSM1-230724/1235
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FSM1-230724/1236
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FSM1-230724/1237
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FSM1-230724/1238
Product: fsm20055					
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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FSM2-230724/1239
Product: fsm20056					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-FSM2-230724/1240
Product: home_hub_100_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-HOME-230724/1241
Product: immersive_home_214_platform					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1242

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 kernel/rootfs image. **CVE ID: CVE-2024-21482**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1243
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1244
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1245
Product: immersive_home_216_platform					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1247
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1248
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1249
Product: immersive_home_316_platform					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1250
Buffer Copy without Checking Size of Input	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-IMME-230724/1251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1252
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1253
Product: immersive_home_318_platform					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1254
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1256
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1257
Product: immersive_home_3210_platform					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1258
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1259
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-IMME-230724/1260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21457	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1261
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1262
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1263
Product: immersive_home_326_platform					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1264
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-IMME-230724/1265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1266
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1267
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1268
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IMME-230724/1269
Product: ipq4018					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-IPQ4-230724/1270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Product: ipq4019					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ4-230724/1271
Product: ipq4028					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ4-230724/1272
Product: ipq4029					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ4-230724/1273
Product: ipq5010					
Affected Version(s): -					
Improper Restriction of	01-Jul-2024	7.8	Memory corruption during the secure boot process, when	https://docs.qualcomm.com/product/publicres	H-QUA-IPQ5-230724/1274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	ources/security bulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1275
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1276
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1277
Product: ipq5028					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the kernel/rootfs image. **CVE ID: CVE-2024-21482**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1279
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1280
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1281
Product: ipq5300					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1282
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while	https://docs.qualcomm.com/product/publicres	H-QUA-IPQ5-230724/1283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1284
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1285
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1286
Product: ipq5302					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1287
Buffer Copy	01-Jul-2024	7.8	Memory corruption when allocating	https://docs.qualcomm.com/pr	H-QUA-IPQ5-230724/1288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	oduct/publicresources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/security bulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1289
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/security bulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1290
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/security bulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1291
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/security bulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1292
Product: ipq5312					
Affected Version(s): -					
Improper Restriction of Operations	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm`	https://docs.qualcomm.com/product/publicresources/security	H-QUA-IPQ5-230724/1293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	bulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1294
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1295
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1296
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1297
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-IPQ5-230724/1298

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21462	2024-bulletin.html	
Product: ipq5332					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1299
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1300
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1301
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1302
Integer Underflow (Wrap or	01-Jul-2024	7.5	Information disclosure while parsing sub-IE	https://docs.qualcomm.com/product/publicres	H-QUA-IPQ5-230724/1303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			length during new IE generation. **CVE ID: CVE-2024-21466**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ5-230724/1304
Product: ipq6000					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ6-230724/1305
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ6-230724/1306
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ6-230724/1307

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ6-230724/1308
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ6-230724/1309
Product: ipq6005					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ6-230724/1310
Product: ipq6010					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ6-230724/1311
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-IPQ6-230724/1312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ6-230724/1313
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ6-230724/1314
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ6-230724/1315
Product: ipq6018					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ6-230724/1316
Buffer Copy without	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicres	H-QUA-IPQ6-230724/1317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ6-230724/1318
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ6-230724/1319
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ6-230724/1320
Product: ipq6028					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ6-230724/1321

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ6-230724/1322
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ6-230724/1323
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ6-230724/1324
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ6-230724/1325
Product: ipq8064					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1326

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: ipq8065					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1327
Product: ipq8068					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1328
Product: ipq8070					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1329
Product: ipq8070a					
Affected Version(s): -					
Improper Restriction of Operations within the	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-IPQ8-230724/1330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1331
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1332
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1333
Product: ipq8071a					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21482		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1335
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1336
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1337
Product: ipq8072a					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1338
Buffer Copy without	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicres	H-QUA-IPQ8-230724/1339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1340
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1341
Product: ipq8074a					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1342
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')					
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1344
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1345
Product: ipq8076					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1346
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1347
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while	https://docs.qualcomm.com/product/publicres	H-QUA-IPQ8-230724/1348

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1349
Product: ipq8076a					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1350
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1351
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1353
Product: ipq8078					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1354
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1355
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1356
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-IPQ8-230724/1357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21458	2024-bulletin.html	
Product: ipq8078a					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1358
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1359
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1360
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1361
Product: ipq8173					
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 Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1362
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1363
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1364
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1365
Product: ipq8174					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-IPQ8-230724/1366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1367
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1368
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ8-230724/1369
Product: ipq9008					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1370

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1371
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1372
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1373
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1374
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1375
Product: ipq9554					
Affected Version(s): -					
Improper Restriction	01-Jul-2024	7.8	Memory corruption during the secure	https://docs.qualcomm.com/pr	H-QUA-IPQ9-230724/1376

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Operations within the Bounds of a Memory Buffer			boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	oduct/publicresources/securitybulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1377
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1378
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1379
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1381
Product: ipq9570					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1382
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1383
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1384
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-IPQ9-230724/1385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21458	2024-bulletin.html	
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1386
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1387
Product: ipq9574					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1388
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1390
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1391
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1392
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-IPQ9-230724/1393
Product: mdm9205s					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-MDM9-230724/1394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-MDM9-230724/1395
Product: mdm9628					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-MDM9-230724/1396
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-MDM9-230724/1397
Product: mdm9640					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-MDM9-230724/1398
Product: mdm9650					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-MDM9-230724/1399
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-MDM9-230724/1400
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-MDM9-230724/1401
Product: msm8996au					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-MSM8-230724/1402
Buffer Copy without Checking Size of Input	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-MSM8-230724/1403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-MSM8-230724/1404
Product: pm8937					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-PM89-230724/1405
Product: pmp8074					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-PMP8-230724/1406
Product: qam8255p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QAM8-230724/1407

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
			context is freed by keymaster. **CVE ID: CVE-2024-21461**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1408
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1409
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1410
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1411
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QAM8-230724/1412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1413
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1414
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1415
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1416
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1417
Product: qam8295p					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1418
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1419
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1420
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1421
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1422

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1423
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1424
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1425
Product: qam8620p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1426
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1428
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1429
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1430
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1431
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1433
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1434
Product: qam8650p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1435
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1436
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1437
Buffer Copy	01-Jul-2024	7.8	Memory corruption when allocating	https://docs.qualcomm.com/pr	H-QUA-QAM8-230724/1438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	oduct/publicresources/security bulletin/july-2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/security bulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1439
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/security bulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1440
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/security bulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1441
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/security bulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1442
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QAM8-230724/1443

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling SA query action frame. **CVE ID: CVE-2024-21458**	bulletin/july-2024-bulletin.html	
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1444
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1445
Product: qam8775p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1446
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1447
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QAM8-230724/1448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1449
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1450
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1451
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1452
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QAM8-230724/1453

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1454
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1455
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAM8-230724/1456
Product: qamsrv1h					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1457
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1459
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1460
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1461
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1462
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1463

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1464
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1465
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1466
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1467
Product: qamsrv1m					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1469
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1470
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1471
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1472
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1473

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1474
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1475
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1476
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1477
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QAMS-230724/1478
Product: qca0000					
Affected Version(s): -					
Buffer Copy without Checking	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCA0-230724/1479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA0-230724/1480
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA0-230724/1481
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA0-230724/1482
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA0-230724/1483
Product: qca4004					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA4-230724/1484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21461	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA4-230724/1485
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA4-230724/1486
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA4-230724/1487
Product: qca4024					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA4-230724/1488
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA4-230724/1489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA4-230724/1490
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA4-230724/1491
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA4-230724/1492
Product: qca6174a					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1493
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA6-230724/1494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1495
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1496
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1497
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1498
Product: qca6234					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA6-230724/1499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context is freed by keymaster. **CVE ID: CVE-2024-21461**	2024-bulletin.html	
Product: qca6310					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1500
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1501
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1502
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1503
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation	https://docs.qualcomm.com/product/publicres	H-QUA-QCA6-230724/1504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	ources/security bulletin/july-2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1505
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1506
Product: qca6320					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1507
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1508
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation	https://docs.qualcomm.com/product/publicres	H-QUA-QCA6-230724/1509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	ources/security bulletin/july-2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1510
Product: qca6335					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1511
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1512
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1513
Buffer Copy without Checking	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCA6-230724/1514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	bulletin/july-2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1515
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1516
Product: qca6391					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1517
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1518
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCA6-230724/1519

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bound for the same trusted application. **CVE ID: CVE-2024-21469**	bulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1520
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1521
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1522
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1523
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCA6-230724/1524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21462	bulletin/july-2024-bulletin.html	
Product: qca6420					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1525
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1526
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1527
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1528
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA6-230724/1529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1530
Product: qca6421					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1531
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1532
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1533
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA6-230724/1534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: qca6426					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1535
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1536
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1537
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1538
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA6-230724/1539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1540
Product: qca6430					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1541
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1542
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1543
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA6-230724/1544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1545
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1546
Product: qca6431					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1547
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1548
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA6-230724/1549

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bound for the same trusted application. **CVE ID: CVE-2024-21469**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1550
Product: qca6436					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1551
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1552
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1553
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA6-230724/1554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1555
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1556
Product: qca6554a					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1557
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1558
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA6-230724/1559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21466	2024-bulletin.html	
Product: qca6564					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1560
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1561
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1562
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1563
Product: qca6564a					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC	https://docs.qualcomm.com/product/publicres	H-QUA-QCA6-230724/1564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1565
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1566
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1567
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1568
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA6-230724/1569

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: qca6564au					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1570
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1571
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1572
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1573
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA6-230724/1574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1575
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1576
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1577
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1578
Product: qca6574					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA6-230724/1579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21461	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1580
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1581
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1582
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1583
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1584

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-23373		
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1585
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1586
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1587
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1588
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1589
Product: qca6574a					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1590
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1591
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1592
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1593
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1594

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1595
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1596
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1597
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1598
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1599
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA6-230724/1600

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: qca6574au					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1601
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1602
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1603
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1604
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA6-230724/1605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			greater than expected size. **CVE ID: CVE-2024-23372**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1606
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1607
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1608
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1609
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1610

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1611
Product: qca6584au					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1612
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1613
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1614
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1615

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1616
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1617
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1618
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1619
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1620
Product: qca6595					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC	https://docs.qualcomm.com/product/publicres	H-QUA-QCA6-230724/1621

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1622
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1623
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1624
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1625
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCA6-230724/1626

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	bulletin/july-2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1627
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1628
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1629
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1630
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1631
Product: qca6595au					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1632
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1633
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1634
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1635
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1636

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
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1637
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1638
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1639
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1640
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1641
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA6-230724/1642

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: qca6678aq					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1643
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1644
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1645
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1646
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA6-230724/1647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			greater than expected size. **CVE ID: CVE-2024-23372**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1648
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1649
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1650
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1651
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1652

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1653
Product: qca6688aq					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1654
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1655
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1656
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1657

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1658
Product: qca6696					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1659
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1660
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1661
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1663
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1664
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1665
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1666
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1667
Integer Underflow (Wrap or	01-Jul-2024	7.5	Information disclosure while parsing sub-IE	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCA6-230724/1668

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			length during new IE generation. **CVE ID: CVE-2024-21466**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1669
Product: qca6698aq					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1670
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1671
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1672
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA6-230724/1673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1674
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1675
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1676
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1677
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA6-230724/1678

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1679
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1680
Product: qca6797aq					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1681
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1682
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1684
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1685
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1686
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1687
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA6-230724/1688
Product: qca7500					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA7-230724/1689
Product: qca8072					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1690
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1691
Product: qca8075					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1692

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21482		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1693
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1694
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1695
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1696
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1697
Product: qca8081					
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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1698
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1699
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1700
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1701
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1702

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')					
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1703
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1704
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1705
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1706
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1707
Product: qca8082					
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 Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1708
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1709
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1710
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1711
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1712

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1713
Product: qca8084					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1714
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1715
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1716
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA8-230724/1717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21458	2024-bulletin.html	
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1718
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1719
Product: qca8085					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1720
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1722
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1723
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1724
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1725
Product: qca8337					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1726

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1727
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1728
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1729
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1730
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1731
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCA8-230724/1732

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling SA query action frame. **CVE ID: CVE-2024-21458**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1733
Product: qca8386					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1734
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1735
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1736

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1737
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1738
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA8-230724/1739
Product: qca9367					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1740
Product: qca9377					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA9-230724/1741

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21461	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1742
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1743
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1744
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1745
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1746
Product: qca9379					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1747
Product: qca9880					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1748
Product: qca9886					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1749
Product: qca9888					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			the kernel/rootfs image. **CVE ID: CVE-2024-21482**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1751
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1752
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1753
Product: qca9889					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1754

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1755
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1756
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1757
Product: qca9898					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1758
Product: qca9980					
Affected Version(s): -					
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCA9-230724/1759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Product: qca9984					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1760
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1761
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1762
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1763
Product: qca9985					
Affected Version(s): -					
Buffer Copy	01-Jul-2024	7.8	Memory corruption when allocating	https://docs.qualcomm.com/pr	H-QUA-QCA9-230724/1764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	oduct/publicresources/security bulletin/july-2024-bulletin.html	
Product: qca9990					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/security bulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1765
Product: qca9992					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/security bulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1766
Product: qca9994					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/security bulletin/july-2024-bulletin.html	H-QUA-QCA9-230724/1767

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: qcc2073					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCC2-230724/1768
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCC2-230724/1769
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCC2-230724/1770
Product: qcc2076					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCC2-230724/1771
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCC2-230724/1772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCC2-230724/1773
Product: qcc710					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCC7-230724/1774
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCC7-230724/1775
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCC7-230724/1776
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCC7-230724/1777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCC7-230724/1778
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCC7-230724/1779
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCC7-230724/1780
Product: qcf8000					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCF8-230724/1781
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCF8-230724/1782

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')					
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCF8-230724/1783
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCF8-230724/1784
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCF8-230724/1785
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCF8-230724/1786
Product: qcf8001					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCF8-230724/1787

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21482		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCF8-230724/1788
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCF8-230724/1789
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCF8-230724/1790
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCF8-230724/1791
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCF8-230724/1792
Product: qcm2150					
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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM2-230724/1793
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM2-230724/1794
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM2-230724/1795
Product: qcm2290					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM2-230724/1796
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCM2-230724/1797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM2-230724/1798
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM2-230724/1799
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM2-230724/1800
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM2-230724/1801
Product: qcm4290					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCM4-230724/1802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context is freed by keymaster. **CVE ID: CVE-2024-21461**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM4-230724/1803
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM4-230724/1804
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM4-230724/1805
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM4-230724/1806
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCM4-230724/1807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: qcm4325					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM4-230724/1808
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM4-230724/1809
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM4-230724/1810
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM4-230724/1811
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCM4-230724/1812

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM4-230724/1813
Product: qcm4490					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM4-230724/1814
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM4-230724/1815
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM4-230724/1816
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCM4-230724/1817

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM4-230724/1818
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM4-230724/1819
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM4-230724/1820
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM4-230724/1821
Product: qcm5430					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCM5-230724/1822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context is freed by keymaster. **CVE ID: CVE-2024-21461**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM5-230724/1823
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM5-230724/1824
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM5-230724/1825
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM5-230724/1826
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCM5-230724/1827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM5-230724/1828
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM5-230724/1829
Product: qcm6125					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM6-230724/1830
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM6-230724/1831
Buffer Copy without Checking Size of Input	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCM6-230724/1832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM6-230724/1833
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM6-230724/1834
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM6-230724/1835
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM6-230724/1836
Product: qcm6490					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCM6-230724/1837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context is freed by keymaster. **CVE ID: CVE-2024-21461**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM6-230724/1838
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM6-230724/1839
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM6-230724/1840
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM6-230724/1841
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCM6-230724/1842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM6-230724/1843
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM6-230724/1844
Product: qcm8550					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM8-230724/1845
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM8-230724/1846
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCM8-230724/1847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM8-230724/1848
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM8-230724/1849
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM8-230724/1850
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM8-230724/1851
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCM8-230724/1852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			one chunk in virtual address space. **CVE ID: CVE-2024-21460**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCM8-230724/1853
Product: qcn5021					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1854
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1855
Product: qcn5022					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21482		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1857
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1858
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1859
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1860
Product: qcn5024					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			the kernel/rootfs image. **CVE ID: CVE-2024-21482**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1862
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1863
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1864
Product: qcn5052					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1865

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1866
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1867
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1868
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1869
Product: qcn5054					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1870

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: qcn5121					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1871
Product: qcn5122					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1872
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1873
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1875
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1876
Product: qcn5124					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1877
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1878
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCN5-230724/1879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21457	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1880
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1881
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1882
Product: qcn5152					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1883
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCN5-230724/1884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1885
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1886
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1887
Product: qcn5154					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1888
Buffer Copy without	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicres	H-QUA-QCN5-230724/1889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1890
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1891
Product: qcn5164					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1892
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')					
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1894
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN5-230724/1895
Product: qcn6023					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1896
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1897
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while	https://docs.qualcomm.com/product/publicres	H-QUA-QCN6-230724/1898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1899
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1900
Product: qcn6024					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1901
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1902
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCN6-230724/1903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1904
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1905
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1906
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1907
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCN6-230724/1908

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21458	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1909
Product: qcn6100					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1910
Product: qcn6102					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1911
Product: qcn6112					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			the kernel/rootfs image. **CVE ID: CVE-2024-21482**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1913
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1914
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1915
Product: qcn6122					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1916

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1917
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1918
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1919
Product: qcn6132					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1920
Buffer Copy without Checking Size of Input	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCN6-230724/1921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1922
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1923
Product: qcn6224					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1924
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1925
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1927
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1928
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1929
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1930
Product: qcn6274					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21461		
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1932
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1933
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1934
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1935
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1936

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1937
Product: qcn6402					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1938
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1939
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1940
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCN6-230724/1941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21458	2024-bulletin.html	
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1942
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1943
Product: qcn6412					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1944
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1946
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1947
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1948
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1949
Product: qcn6422					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1950

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1951
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1952
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1953
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1954
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1955
Product: qcn6432					
Affected Version(s): -					
Improper Restriction	01-Jul-2024	7.8	Memory corruption during the secure	https://docs.qualcomm.com/pr	H-QUA-QCN6-230724/1956

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Operations within the Bounds of a Memory Buffer			boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	oduct/publicresources/securitybulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1957
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1958
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1959
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1960

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN6-230724/1961
Product: qcn7606					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN7-230724/1962
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN7-230724/1963
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN7-230724/1964
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN7-230724/1965
Product: qcn9000					
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 Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1966
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1967
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1968
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1969
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1970

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1971
Product: qcn9001					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1972
Product: qcn9002					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1973
Product: qcn9003					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcn9011					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1975
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1976
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1977
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1978
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1979

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1980
Product: qcn9012					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1981
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1982
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1983
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1985
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1986
Product: qcn9013					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1987
Product: qcn9022					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1988
Buffer Copy without	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicres	H-QUA-QCN9-230724/1989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1990
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1991
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1992
Product: qcn9024					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1993
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCN9-230724/1994

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21465	bulletin/july-2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1995
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1996
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1997
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/1998
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while	https://docs.qualcomm.com/product/publicres	H-QUA-QCN9-230724/1999

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2000
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2001
Product: qcn9070					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2002
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2004
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2005
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2006
Product: qcn9072					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2007
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2008

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')					
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2009
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2010
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2011
Product: qcn9074					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2012
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the kernel/rootfs image. **CVE ID: CVE-2024-21482**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2014
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2015
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2016
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2017
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2018

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: qcn9100					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2019
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2020
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2021
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2022
Product: qcn9274					
Affected Version(s): -					
Improper Restriction of	01-Jul-2024	7.8	Memory corruption during the secure boot process, when	https://docs.qualcomm.com/product/publicres	H-QUA-QCN9-230724/2023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	ources/security bulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2024
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2025
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2026
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCN9-230724/2027
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCN9-230724/2028

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21462	bulletin/july-2024-bulletin.html	
Product: qcs2290					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS2-230724/2029
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS2-230724/2030
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS2-230724/2031
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS2-230724/2032
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCS2-230724/2033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS2-230724/2034
Product: qcs410					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS4-230724/2035
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS4-230724/2036
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS4-230724/2037
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCS4-230724/2038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS4-230724/2039
Product: qcs4290					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS4-230724/2040
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS4-230724/2041
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS4-230724/2042
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCS4-230724/2043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS4-230724/2044
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS4-230724/2045
Product: qcs4490					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS4-230724/2046
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS4-230724/2047
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCS4-230724/2048

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bound for the same trusted application. **CVE ID: CVE-2024-21469**	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS4-230724/2049
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS4-230724/2050
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS4-230724/2051
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS4-230724/2052
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCS4-230724/2053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21462	bulletin/july-2024-bulletin.html	
Product: qcs5430					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS5-230724/2054
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS5-230724/2055
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS5-230724/2056
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS5-230724/2057
Integer Overflow or	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCS5-230724/2058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			greater than expected size. **CVE ID: CVE-2024-23372**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS5-230724/2059
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS5-230724/2060
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS5-230724/2061
Product: qcs610					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS6-230724/2062
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCS6-230724/2063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	bulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS6-230724/2064
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS6-230724/2065
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS6-230724/2066
Product: qcs6125					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS6-230724/2067
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCS6-230724/2068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			key blob passed by the user. **CVE ID: CVE-2024-21465**	bulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS6-230724/2069
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS6-230724/2070
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS6-230724/2071
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS6-230724/2072
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCS6-230724/2073

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21462	bulletin/july-2024-bulletin.html	
Product: qcs6490					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS6-230724/2074
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS6-230724/2075
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS6-230724/2076
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS6-230724/2077
Integer Overflow or	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCS6-230724/2078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			greater than expected size. **CVE ID: CVE-2024-23372**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS6-230724/2079
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS6-230724/2080
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS6-230724/2081
Product: qcs7230					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS7-230724/2082
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCS7-230724/2083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	bulletin/july-2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS7-230724/2084
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS7-230724/2085
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS7-230724/2086
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS7-230724/2087
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCS7-230724/2088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-23380	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS7-230724/2089
Product: qcs8155					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS8-230724/2090
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS8-230724/2091
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS8-230724/2092
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS8-230724/2093

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: qcs8250					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS8-230724/2094
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS8-230724/2095
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS8-230724/2096
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS8-230724/2097
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS8-230724/2098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-23372		
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS8-230724/2099
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS8-230724/2100
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS8-230724/2101
Product: qcs8550					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS8-230724/2102
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCS8-230724/2103

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS8-230724/2104
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS8-230724/2105
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS8-230724/2106
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS8-230724/2107
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QCS8-230724/2108

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS8-230724/2109
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QCS8-230724/2110
Product: qdu1000					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDU1-230724/2111
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDU1-230724/2112
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QDU1-230724/2113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDU1-230724/2114
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDU1-230724/2115
Product: qdu1010					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDU1-230724/2116
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDU1-230724/2117
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QDU1-230724/2118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDU1-230724/2119
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDU1-230724/2120
Product: qdu1110					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDU1-230724/2121
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDU1-230724/2122
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QDU1-230724/2123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDU1-230724/2124
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDU1-230724/2125
Product: qdu1210					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDU1-230724/2126
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDU1-230724/2127
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QDU1-230724/2128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDU1-230724/2129
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDU1-230724/2130
Product: qdx1010					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDX1-230724/2131
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDX1-230724/2132
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QDX1-230724/2133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDX1-230724/2134
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDX1-230724/2135
Product: qdx1011					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDX1-230724/2136
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDX1-230724/2137
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QDX1-230724/2138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDX1-230724/2139
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QDX1-230724/2140
Product: qep8111					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QEP8-230724/2141
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QEP8-230724/2142
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QEP8-230724/2143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QEP8-230724/2144
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QEP8-230724/2145
Product: qfw7114					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QFW7-230724/2146
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QFW7-230724/2147
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-QFW7-230724/2148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QFW7-230724/2149
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QFW7-230724/2150
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QFW7-230724/2151
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QFW7-230724/2152
Product: qfw7124					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QFW7-230724/2153

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21461		
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QFW7-230724/2154
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QFW7-230724/2155
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QFW7-230724/2156
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QFW7-230724/2157
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QFW7-230724/2158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QFW7-230724/2159
Product: qrb5165m					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRB5-230724/2160
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRB5-230724/2161
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRB5-230724/2162
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRB5-230724/2163

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRB5-230724/2164
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRB5-230724/2165
Product: qrb5165n					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRB5-230724/2166
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRB5-230724/2167
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRB5-230724/2168

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRB5-230724/2169
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRB5-230724/2170
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRB5-230724/2171
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRB5-230724/2172
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRB5-230724/2173
Product: qru1032					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRU1-230724/2174
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRU1-230724/2175
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRU1-230724/2176
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRU1-230724/2177
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRU1-230724/2178
Product: qru1052					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRU1-230724/2179
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRU1-230724/2180
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRU1-230724/2181
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRU1-230724/2182
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRU1-230724/2183
Product: qru1062					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRU1-230724/2184
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRU1-230724/2185
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRU1-230724/2186
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRU1-230724/2187
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QRU1-230724/2188
Product: qsm8250					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QSM8-230724/2189
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QSM8-230724/2190
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QSM8-230724/2191
Product: qsm8350					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QSM8-230724/2192
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QSM8-230724/2193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QSM8-230724/2194
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QSM8-230724/2195
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QSM8-230724/2196
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QSM8-230724/2197
Product: qts110					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QTS1-230724/2198

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QTS1-230724/2199
Product: qualcomm_205_mobile_platform					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QUAL-230724/2200
Product: qualcomm_215_mobile_platform					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-QUAL-230724/2201
Product: robotics_rb3_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-ROBO-230724/2202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-ROBO-230724/2203
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-ROBO-230724/2204
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-ROBO-230724/2205
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-ROBO-230724/2206
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-ROBO-230724/2207
Product: robotics_rb5_platform					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-ROBO-230724/2208
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-ROBO-230724/2209
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-ROBO-230724/2210
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-ROBO-230724/2211
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-ROBO-230724/2212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-ROBO-230724/2213
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-ROBO-230724/2214
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-ROBO-230724/2215
Product: sa4150p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA41-230724/2216
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA41-230724/2217

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA41-230724/2218
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA41-230724/2219
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA41-230724/2220
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA41-230724/2221
Product: sa4155p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA41-230724/2222

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA41-230724/2223
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA41-230724/2224
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA41-230724/2225
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA41-230724/2226
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA41-230724/2227
Product: sa6145p					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2228
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2229
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2230
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2231
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2233
Product: sa6150p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2234
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2235
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2236
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2238
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2239
Product: sa6155					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2240
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2241
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2242

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2243
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2244
Product: sa6155p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2245
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2246
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2247

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2248
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2249
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2250
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2251
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA61-230724/2252
Product: sa7255p					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA72-230724/2253
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA72-230724/2254
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA72-230724/2255
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA72-230724/2256
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA72-230724/2257

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA72-230724/2258
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA72-230724/2259
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA72-230724/2260
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA72-230724/2261
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA72-230724/2262
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SA72-230724/2263

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: sa7775p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA77-230724/2264
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA77-230724/2265
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA77-230724/2266
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA77-230724/2267
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SA77-230724/2268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			greater than expected size. **CVE ID: CVE-2024-23372**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA77-230724/2269
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA77-230724/2270
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA77-230724/2271
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA77-230724/2272
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA77-230724/2273

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA77-230724/2274
Product: sa8145p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2275
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2276
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2277
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2279
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2280
Product: sa8150p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2281
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2282
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2283

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2284
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2285
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2286
Product: sa8155					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2287
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2288

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2289
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2290
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2291
Product: sa8155p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2292
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2294
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2295
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2296
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2297
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2299
Product: sa8195p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2300
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2301
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2302
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2304
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2305
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2306
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA81-230724/2307
Product: sa8255p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA82-230724/2308

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA82-230724/2309
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA82-230724/2310
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA82-230724/2311
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA82-230724/2312
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA82-230724/2313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA82-230724/2314
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA82-230724/2315
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA82-230724/2316
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA82-230724/2317
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA82-230724/2318
Product: sa8295p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SA82-230724/2319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context is freed by keymaster. **CVE ID: CVE-2024-21461**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA82-230724/2320
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA82-230724/2321
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA82-230724/2322
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA82-230724/2323
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SA82-230724/2324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA82-230724/2325
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA82-230724/2326
Product: sa8530p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA85-230724/2327
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA85-230724/2328
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SA85-230724/2329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA85-230724/2330
Product: sa8540p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA85-230724/2331
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA85-230724/2332
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA85-230724/2333
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SA85-230724/2334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA85-230724/2335
Product: sa8620p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2336
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2337
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2338
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SA86-230724/2339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2340
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2341
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2342
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2343
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SA86-230724/2344

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2345
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2346
Product: sa8650p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2347
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2348
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2350
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2351
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2352
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2353
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2354

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2355
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2356
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA86-230724/2357
Product: sa8770p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2358
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2359

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2360
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2361
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2362
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2363
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2365
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2366
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2367
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2368
Product: sa8775p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2369

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2370
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2371
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2372
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2373
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2374

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2375
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2376
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2377
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2378
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA87-230724/2379
Product: sa9000p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SA90-230724/2380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context is freed by keymaster. **CVE ID: CVE-2024-21461**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA90-230724/2381
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA90-230724/2382
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA90-230724/2383
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA90-230724/2384
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SA90-230724/2385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA90-230724/2386
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA90-230724/2387
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA90-230724/2388
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA90-230724/2389
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SA90-230724/2390
Product: sc7180-ac					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC71-230724/2391
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC71-230724/2392
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC71-230724/2393
Product: sc7180-ad					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC71-230724/2394
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC71-230724/2395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC71-230724/2396
Product: sc8180x-aa					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2397
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2398
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2399
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2400
Product: sc8180x-ab					
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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2401
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2402
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2403
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2404
Product: sc8180x-ac					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2405

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2406
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2407
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2408
Product: sc8180x-ad					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2409
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2411
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2412
Product: sc8180x-af					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2413
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2414
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2415

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2416
Product: sc8180xp-aa					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2417
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2418
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2419
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2420
Product: sc8180xp-ab					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2421
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2422
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2423
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2424
Product: sc8180xp-ac					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2425

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2426
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2427
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2428
Product: sc8180xp-ad					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2429
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2431
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2432
Product: sc8180xp-af					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2433
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2434
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2436
Product: sc8180x\+sdx55					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2437
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC81-230724/2438
Product: sc8280xp-ab					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC82-230724/2439
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SC82-230724/2440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC82-230724/2441
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC82-230724/2442
Product: sc8280xp-bb					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC82-230724/2443
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC82-230724/2444
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC82-230724/2445

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC82-230724/2446
Product: sc8380xp					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC83-230724/2447
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC83-230724/2448
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC83-230724/2449
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SC83-230724/2450
Product: sd460					
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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD46-230724/2451
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD46-230724/2452
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD46-230724/2453
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD46-230724/2454
Product: sd626					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD62-230724/2455
Product: sd660					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD66-230724/2456
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD66-230724/2457
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD66-230724/2458
Product: sd662					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD66-230724/2459
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SD66-230724/2460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	bulletin/july-2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD66-230724/2461
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD66-230724/2462
Product: sd670					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD67-230724/2463
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD67-230724/2464
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SD67-230724/2465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD67-230724/2466
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD67-230724/2467
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD67-230724/2468
Product: sd675					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD67-230724/2469
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SD67-230724/2470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD67-230724/2471
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD67-230724/2472
Product: sd730					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD73-230724/2473
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD73-230724/2474
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD73-230724/2475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')					
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD73-230724/2476
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD73-230724/2477
Product: sd820					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD82-230724/2478
Product: sd821					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD82-230724/2479
Product: sd835					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD83-230724/2480
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD83-230724/2481
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD83-230724/2482
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD83-230724/2483
Product: sd855					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD85-230724/2484

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21461		
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD85-230724/2485
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD85-230724/2486
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD85-230724/2487
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD85-230724/2488
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD85-230724/2489
Product: sd865_5g					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD86-230724/2490
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD86-230724/2491
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD86-230724/2492
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD86-230724/2493
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD86-230724/2494

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD86-230724/2495
Product: sd888					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD88-230724/2496
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD88-230724/2497
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD88-230724/2498
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD88-230724/2499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-23372		
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD88-230724/2500
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD88-230724/2501
Product: sdm429w					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SDM4-230724/2502
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SDM4-230724/2503
Product: sdx55					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing	https://docs.qualcomm.com/pr	H-QUA-SDX5-230724/2504

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	oduct/publicresources/securitybulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SDX5-230724/2505
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SDX5-230724/2506
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SDX5-230724/2507
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SDX5-230724/2508

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SDX5-230724/2509
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SDX5-230724/2510
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SDX5-230724/2511
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SDX5-230724/2512
Product: sdx57m					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SDX5-230724/2513
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are	https://docs.qualcomm.com/product/publicres	H-QUA-SDX5-230724/2514

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bound for the same trusted application. **CVE ID: CVE-2024-21469**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SDX5-230724/2515
Product: sdx65m					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SDX6-230724/2516
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SDX6-230724/2517
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SDX6-230724/2518

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SDX6-230724/2519
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SDX6-230724/2520
Product: sdx71m					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SDX7-230724/2521
Product: sd_455					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD_4-230724/2522
Product: sd_675					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SD_6-230724/2523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context is freed by keymaster. **CVE ID: CVE-2024-21461**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD_6-230724/2524
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD_6-230724/2525
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD_6-230724/2526
Product: sd_8cx					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD_8-230724/2527
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SD_8-230724/2528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD_8-230724/2529
Product: sd_8_gen1_5g					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD_8-230724/2530
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD_8-230724/2531
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD_8-230724/2532
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD_8-230724/2533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')					
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD_8-230724/2534
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD_8-230724/2535
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD_8-230724/2536
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SD_8-230724/2537
Product: sg4150p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SG41-230724/2538

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
			context is freed by keymaster. **CVE ID: CVE-2024-21461**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SG41-230724/2539
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SG41-230724/2540
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SG41-230724/2541
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SG41-230724/2542
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SG41-230724/2543

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-2024-23380	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SG41-230724/2544
Product: sg8275p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SG82-230724/2545
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SG82-230724/2546
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SG82-230724/2547
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SG82-230724/2548

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SG82-230724/2549
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SG82-230724/2550
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SG82-230724/2551
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SG82-230724/2552
Product: sm4125					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC	https://docs.qualcomm.com/product/publicres	H-QUA-SM41-230724/2553

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
			operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM41-230724/2554
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM41-230724/2555
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM41-230724/2556
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM41-230724/2557
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SM41-230724/2558

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: sm4350-ac					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM43-230724/2559
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM43-230724/2560
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM43-230724/2561
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM43-230724/2562
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SM43-230724/2563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			greater than expected size. **CVE ID: CVE-2024-23372**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM43-230724/2564
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM43-230724/2565
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM43-230724/2566
Product: sm6150-ac					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM61-230724/2567
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SM61-230724/2568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	bulletin/july-2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM61-230724/2569
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM61-230724/2570
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM61-230724/2571
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM61-230724/2572
Product: sm6225-ad					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SM62-230724/2573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context is freed by keymaster. **CVE ID: CVE-2024-21461**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM62-230724/2574
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM62-230724/2575
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM62-230724/2576
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM62-230724/2577
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SM62-230724/2578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM62-230724/2579
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM62-230724/2580
Product: sm6250					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM62-230724/2581
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM62-230724/2582
Buffer Copy without Checking Size of Input	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SM62-230724/2583

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM62-230724/2584
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM62-230724/2585
Product: sm6250p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM62-230724/2586
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM62-230724/2587
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SM62-230724/2588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: sm6370					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM63-230724/2589
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM63-230724/2590
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM63-230724/2591
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM63-230724/2592
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SM63-230724/2593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM63-230724/2594
Product: sm7150-aa					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM71-230724/2595
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM71-230724/2596
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM71-230724/2597
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SM71-230724/2598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM71-230724/2599
Product: sm7150-ab					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM71-230724/2600
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM71-230724/2601
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM71-230724/2602
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SM71-230724/2603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM71-230724/2604
Product: sm7150-ac					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM71-230724/2605
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM71-230724/2606
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM71-230724/2607
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SM71-230724/2608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM71-230724/2609
Product: sm7250-aa					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2610
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2611
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2612
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SM72-230724/2613

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2614
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2615
Product: sm7250-ab					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2616
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2617
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SM72-230724/2618

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bound for the same trusted application. **CVE ID: CVE-2024-21469**	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2619
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2620
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2621
Product: sm7250-ac					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2623
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2624
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2625
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2626
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2627
Product: sm7250p					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2628
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2629
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2630
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2631
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM72-230724/2633
Product: sm7315					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2634
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2635
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2636
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-23372		
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2638
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2639
Product: sm7325-ae					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2640
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2641
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SM73-230724/2642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2643
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2644
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2645
Product: sm7325-af					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2646
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SM73-230724/2647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	bulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2648
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2649
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2650
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2651
Product: sm7325p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC	https://docs.qualcomm.com/product/publicres	H-QUA-SM73-230724/2652

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2653
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2654
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2655
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM73-230724/2656
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file.	https://docs.qualcomm.com/product/publicres	H-QUA-SM73-230724/2657

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21462	ources/security bulletin/july-2024-bulletin.html	
Product: sm8150-ac					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM81-230724/2658
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM81-230724/2659
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM81-230724/2660
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM81-230724/2661
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SM81-230724/2662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM81-230724/2663
Product: sm8250-ab					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM82-230724/2664
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM82-230724/2665
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM82-230724/2666
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SM82-230724/2667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM82-230724/2668
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM82-230724/2669
Product: sm8250-ac					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM82-230724/2670
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM82-230724/2671
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SM82-230724/2672

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bound for the same trusted application. **CVE ID: CVE-2024-21469**	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM82-230724/2673
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM82-230724/2674
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM82-230724/2675
Product: sm8350-ac					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM83-230724/2676

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM83-230724/2677
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM83-230724/2678
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM83-230724/2679
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM83-230724/2680
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM83-230724/2681

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM83-230724/2682
Product: sm8550p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM85-230724/2683
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM85-230724/2684
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM85-230724/2685
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM85-230724/2686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM85-230724/2687
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM85-230724/2688
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM85-230724/2689
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM85-230724/2690
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SM85-230724/2691
Product: smart_audio_400_platform					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SMAR-230724/2692
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SMAR-230724/2693
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SMAR-230724/2694
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SMAR-230724/2695
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SMAR-230724/2696

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SMAR-230724/2697
Product: snapdragon_210_processor					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2698
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2699
Product: snapdragon_212_mobile_platform					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2700
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SNAP-230724/2701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	bulletin/july-2024-bulletin.html	
Product: snapdragon_425_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2702
Product: snapdragon_427_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2703
Product: snapdragon_429_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2704
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SNAP-230724/2705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Product: snapdragon_430_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2706
Product: snapdragon_435_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2707
Product: snapdragon_439_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2708
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SNAP-230724/2709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Product: snapdragon_450_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2710
Product: snapdragon_460_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2711
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2712
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2714
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2715
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2716
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2717
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2718
Product: snapdragon_480_5g_mobile_platform					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2719
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2720
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2721
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2722
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2723

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
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2724
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2725
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2726
Product: snapdragon_4_gen_1_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2727
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2729
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2730
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2731
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2732
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2734
Product: snapdragon_4_gen_2_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2735
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2736
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2737
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2738

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2739
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2740
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2741
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2742
Product: snapdragon_625_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2743

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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_626_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2744
Product: snapdragon_630_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2745
Product: snapdragon_632_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2746
Product: snapdragon_636_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2747

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-2024-21461		
Product: snapdragon_660_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2748
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2749
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2750
Product: snapdragon_662_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2752
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2753
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2754
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2755
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2756

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2757
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2758
Product: snapdragon_665_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2759
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2760
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2762
Product: snapdragon_670_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2763
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2764
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2765
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2767
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2768
Product: snapdragon_675_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2769
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2770
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2772
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2773
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2774
Product: snapdragon_680_4g_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2775
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2776

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2777
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2778
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2779
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2780
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2782
Product: snapdragon_690_5g_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2783
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2784
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2785
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2787
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2788
Product: snapdragon_695_5g_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2789
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2790
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2792
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2793
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2794
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2795
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2796
Product: snapdragon_710_mobile_platform					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2797
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2798
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2799
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2800
Product: snapdragon_712_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SNAP-230724/2801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context is freed by keymaster. **CVE ID: CVE-2024-21461**	2024-bulletin.html	
Product: snapdragon_720g_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2802
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2803
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2804
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2806
Product: snapdragon_750g_5g_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2807
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2808
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2809
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2810

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2811
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2812
Product: snapdragon_778g_5g_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2813
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2814
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2815

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
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2816
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2817
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2818
Product: snapdragon_780g_5g_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2819
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2820

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2821
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2822
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2823
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2824
Product: snapdragon_7c\+_gen_3_compute					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SNAP-230724/2825

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21461	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2826
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2827
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2828
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2829
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SNAP-230724/2830

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: snapdragon_820_automotive_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2831
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2832
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2833
Product: snapdragon_820_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_821_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2835
Product: snapdragon_835_mobile_pc_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2836
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2837
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2838
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-230724/2839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packets during VBO bind operation. **CVE ID: CVE-2024-23380**	ources/security bulletin/july-2024-bulletin.html	
Product: snapdragon_845_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2840
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2841
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2842
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2843
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-230724/2844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2845
Product: snapdragon_850_mobile_compute_platform					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2846
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2847
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2848
Product: snapdragon_855_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-230724/2849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2850
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2851
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2852
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2853
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SNAP-230724/2854

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: snapdragon_865_5g_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2855
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2856
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2857
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2858
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SNAP-230724/2859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2860
Product: snapdragon_888_5g_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2861
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2862
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2863
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SNAP-230724/2864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2865
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2866
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2867
Product: snapdragon_8\+_gen_1_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2869
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2870
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2871
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2872
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2873

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
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2874
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2875
Product: snapdragon_8\+_gen_2_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2876
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2877
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2878
Buffer Copy without	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-230724/2879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	ources/security bulletin/july-2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2880
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2881
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2882
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2883

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2884
Product: snapdragon_8_gen_1_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2885
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2886
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2887
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2889
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2890
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2891
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2892
Product: snapdragon_8_gen_2_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2893

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2894
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2895
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2896
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2897
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2898

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2899
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2900
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2901
Product: snapdragon_8_gen_3_mobile_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2902
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2903

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
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2904
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2905
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2906
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2907
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2909
Product: snapdragon_ar2_gen_1_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2910
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2911
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2912
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2913

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
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2914
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2915
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2916
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2917
Product: snapdragon_auto_4g_modem					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2918

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2919
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2920
Product: snapdragon_auto_5g_modem-rf					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2921
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2922
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SNAP-230724/2923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-23373	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2924
Product: snapdragon_auto_5g_modem-rf_gen_2					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2925
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2926
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2927
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')					
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2929
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2930
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2931
Product: snapdragon_w5\+_gen_1_wearable_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2932
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2933

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2934
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2935
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2936
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2937
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2938
Product: snapdragon_wear_1300_platform					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2939
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2940
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2941
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2942
Product: snapdragon_wear_4100\+_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2943

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2944
Product: snapdragon_x12_lte_modem					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2945
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2946
Product: snapdragon_x24_lte_modem					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2947
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-230724/2948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			key blob passed by the user. **CVE ID: CVE-2024-21465**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2949
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2950
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2951
Product: snapdragon_x35_5g_modem-rf_system					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2952
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-230724/2953

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			key blob passed by the user. **CVE ID: CVE-2024-21465**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2954
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2955
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2956
Product: snapdragon_x50_5g_modem-rf_system					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2957
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-230724/2958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			key blob passed by the user. **CVE ID: CVE-2024-21465**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2959
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2960
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2961
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2962
Product: snapdragon_x55_5g_modem-rf_system					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-230724/2963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2964
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2965
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2966
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2967
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SNAP-230724/2968

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
				2024-bulletin.html	
Product: snapdragon_x62_5g_modem-rf_system					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2969
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2970
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2971
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2972
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SNAP-230724/2973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2974
Product: snapdragon_x65_5g_modem-rf_system					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2975
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2976
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2977
Improper Restriction of Operations within the	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SNAP-230724/2978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2979
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2980
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2981
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2982
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SNAP-230724/2983

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21462	2024-bulletin.html	
Product: snapdragon_x70_modem-rf_system					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2984
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2985
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2986
Product: snapdragon_x72_5g_modem-rf_system					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2987
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SNAP-230724/2988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2989
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2990
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2991
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2992
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2993
Product: snapdragon_x75_5g_modem-rf_system					
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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2994
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2995
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2996
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2997
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/2998
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SNAP-230724/2999

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling SA query action frame. **CVE ID: CVE-2024-21458**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/3000
Product: snapdragon_xr1_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/3001
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/3002
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/3003
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SNAP-230724/3004

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
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	bulletin/july-2024-bulletin.html	
Product: snapdragon_xr2\+_gen_1_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/3005
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/3006
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/3007
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/3008
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-230724/3009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/3010
Product: snapdragon_xr2_5g_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/3011
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/3012
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/3013
Buffer Copy without Checking	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SNAP-230724/3014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	bulletin/july-2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/3015
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SNAP-230724/3016
Product: srv1h					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3017
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3018
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SRV1-230724/3019

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bound for the same trusted application. **CVE ID: CVE-2024-21469**	bulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3020
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3021
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3022
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3023
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SRV1-230724/3024

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21457	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3025
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3026
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3027
Product: srv1l					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3028
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SRV1-230724/3029

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
				2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3030
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3031
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3032
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3033
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-SRV1-230724/3034

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3035
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3036
Product: srv1m					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3037
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3038
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3040
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3041
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3042
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3043
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3044

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3045
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3046
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SRV1-230724/3047
Product: ssg2115p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SSG2-230724/3048
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SSG2-230724/3049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SSG2-230724/3050
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SSG2-230724/3051
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SSG2-230724/3052
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SSG2-230724/3053
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SSG2-230724/3054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SSG2-230724/3055
Product: ssg2125p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SSG2-230724/3056
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SSG2-230724/3057
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SSG2-230724/3058
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SSG2-230724/3059

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
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SSG2-230724/3060
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SSG2-230724/3061
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SSG2-230724/3062
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SSG2-230724/3063
Product: sw5100					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SW51-230724/3064

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
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SW51-230724/3065
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SW51-230724/3066
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SW51-230724/3067
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SW51-230724/3068
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SW51-230724/3069

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
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SW51-230724/3070
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SW51-230724/3071
Product: sw5100p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SW51-230724/3072
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SW51-230724/3073
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SW51-230724/3074

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SW51-230724/3075
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SW51-230724/3076
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SW51-230724/3077
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SW51-230724/3078
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SW51-230724/3079
Product: sxr1120					
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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR1-230724/3080
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR1-230724/3081
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR1-230724/3082
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR1-230724/3083
Product: sxr1230p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR1-230724/3084

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21461		
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR1-230724/3085
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR1-230724/3086
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR1-230724/3087
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR1-230724/3088
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR1-230724/3089

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-23373		
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR1-230724/3090
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR1-230724/3091
Product: sxr2130					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3092
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3093
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3094

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3095
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3096
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3097
Product: sxr2230p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3098
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3099

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3100
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3101
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3102
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3103
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3104

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3105
Product: sxr2250p					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3106
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3107
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3108
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3109

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3110
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3111
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3112
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-SXR2-230724/3113
Product: talynplus					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-TALY-230724/3114

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-TALY-230724/3115
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-TALY-230724/3116
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-TALY-230724/3117
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-TALY-230724/3118
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-TALY-230724/3119

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-TALY-230724/3120
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-TALY-230724/3121
Product: video_collaboration_vc1_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3122
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3123
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3125
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3126
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3127
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3128
Product: video_collaboration_vc3_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3129

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3130
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3131
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3132
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3133
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3134

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3135
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3136
Product: video_collaboration_vc5_platform					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3137
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3138
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3139
Buffer Copy without	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicres	H-QUA-VIDE-230724/3140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	ources/security bulletin/july-2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3141
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3142
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3143
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VIDE-230724/3144
Product: vision_intelligence_300_platform					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VISI-230724/3145
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VISI-230724/3146
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VISI-230724/3147
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VISI-230724/3148
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VISI-230724/3149
Product: vision_intelligence_400_platform					
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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VISI-230724/3150
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VISI-230724/3151
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VISI-230724/3152
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VISI-230724/3153
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VISI-230724/3154

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-VISI-230724/3155
Product: wcd9306					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3156
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3157
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3158
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3159
Product: wcd9326					
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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3160
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3161
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3162
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3163
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3165
Product: wcd9335					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3166
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3167
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3168
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3169

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3170
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3171
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3172
Product: wcd9340					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3173
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3175
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3176
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3177
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3178
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3179
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WCD9-230724/3180

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling SA query action frame. **CVE ID: CVE-2024-21458**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3181
Product: wcd9341					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3182
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3183
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3184
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-WCD9-230724/3185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3186
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3187
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3188
Product: wcd9360					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3189
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-WCD9-230724/3190

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21462	2024-bulletin.html	
Product: wcd9370					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3191
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3192
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3193
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3194
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-WCD9-230724/3195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			greater than expected size. **CVE ID: CVE-2024-23372**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3196
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3197
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3198
Product: wcd9371					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3199
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WCD9-230724/3200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3201
Product: wcd9375					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3202
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3203
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3204
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-WCD9-230724/3205

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3206
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3207
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3208
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3209
Product: wcd9380					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-WCD9-230724/3210

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 is freed by keymaster. **CVE ID: CVE-2024-21461**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3211
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3212
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3213
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3214
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-WCD9-230724/3215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3216
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3217
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3218
Product: wcd9385					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3219
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	H-QUA-WCD9-230724/3220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			key blob passed by the user. **CVE ID: CVE-2024-21465**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3221
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3222
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3223
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3224
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WCD9-230724/3225

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
			CVE ID: CVE-2024-23380	bulletin/july-2024-bulletin.html	
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3226
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3227
Product: wcd9390					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3228
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3229
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	H-QUA-WCD9-230724/3230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bound for the same trusted application. **CVE ID: CVE-2024-21469**	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3231
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3232
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3233
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3234
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WCD9-230724/3235

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3236
Product: wcd9395					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3237
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3238
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3239
Buffer Copy without Checking	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WCD9-230724/3240

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
Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	bulletin/july-2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3241
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3242
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3243
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCD9-230724/3244
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file.	https://docs.qualcomm.com/product/publicres	H-QUA-WCD9-230724/3245

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
			CVE ID: CVE-2024-21462	ources/security bulletin/july-2024-bulletin.html	
Product: wcn3610					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3246
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3247
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3248
Product: wcn3615					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21461		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3250
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3251
Product: wcn3620					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3252
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3253
Product: wcn3660					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3254
Product: wcn3660b					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3255
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3256
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3257
Product: wcn3680					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC	https://docs.qualcomm.com/product/publicres	H-QUA-WCN3-230724/3258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	ources/security bulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3259
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3260
Product: wcn3680b					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3261
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3262

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3263
Product: wcn3910					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3264
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3265
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3266
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3267

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3268
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3269
Product: wcn3950					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3270
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3271
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3272

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3273
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3274
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3275
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3276
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3277
Product: wcn3980					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3278
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3279
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3280
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3281
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3282

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
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3283
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3284
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3285
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3286
Product: wcn3988					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3287

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3288
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3289
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3290
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3291
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3292

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3293
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3294
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3295
Product: wcn3990					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3296
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3298
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3299
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3300
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3301
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3302
Product: wcn3999					
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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3303
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3304
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3305
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN3-230724/3306
Product: wcn6740					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN6-230724/3307

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
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN6-230724/3308
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN6-230724/3309
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN6-230724/3310
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN6-230724/3311
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WCN6-230724/3312
Product: wsa8810					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3313
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3314
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3315
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3316
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3317

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3318
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3319
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3320
Product: wsa8815					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3321
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3323
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3324
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3325
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3326
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3328
Product: wsa8830					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3329
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3330
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3331
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3332

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
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3333
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3334
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3335
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3336
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3337
Product: wsa8832					
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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3338
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3339
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3340
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3341
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3342

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
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3343
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3344
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3345
Product: wsa8835					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3346
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3347

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3348
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3349
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3350
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3351
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3353
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3354
Product: wsa8840					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3355
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3356
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3357
Buffer Copy	01-Jul-2024	7.8	Memory corruption when allocating	https://docs.qualcomm.com/pr	H-QUA-WSA8-230724/3358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	oduct/publicresources/securitybulletin/july-2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3359
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3360
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3361
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3362

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3363
Product: wsa8845					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3364
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3365
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3366
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3367

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3368
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3369
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3370
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3371
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3372
Product: wsa8845h					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3373
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3374
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3375
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3376
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3377

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
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3378
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3379
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3380
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	H-QUA-WSA8-230724/3381
Vendor: Samsung					
Product: exynos_1080					
Affected Version(s): -					
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/,	H-SAM-EXYN-230724/3382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos 1280, Exynos 1380, Exynos 1330, and Exynos W930 where they do not properly check length of the data, which can lead to a Denial of Service. **CVE ID: CVE-2024-27360**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27360/	
Product: exynos_1280					
Affected Version(s): -					
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, and Exynos W930 where they do not properly check length of the data, which can lead to a Denial of Service. **CVE ID: CVE-2024-27360**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27360/	H-SAM-EXYN-230724/3383
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 1280, Exynos 2200, Exynos 1330, Exynos 1380, and Exynos 2400 where they do not properly check the length of the data,	https://semiconductor.samsung.com/support/quality-	H-SAM-EXYN-230724/3384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which can lead to a Information disclosure. **CVE ID: CVE-2024-27362**	support/product-security-updates/cve-2024-27362/	
Product: exynos_1330					
Affected Version(s): -					
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, and Exynos W930 where they do not properly check length of the data, which can lead to a Denial of Service. **CVE ID: CVE-2024-27360**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27360/	H-SAM-EXYN-230724/3385
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 1280, Exynos 2200, Exynos 1330, Exynos 1380, and Exynos 2400 where they do not properly check the length of the data, which can lead to a Information disclosure. **CVE ID: CVE-2024-27362**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27362/	H-SAM-EXYN-230724/3386

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
Product: exynos_1380					
Affected Version(s): -					
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, and Exynos W930 where they do not properly check length of the data, which can lead to a Denial of Service. **CVE ID: CVE-2024-27360**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27360/	H-SAM-EXYN-230724/3387
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 1280, Exynos 2200, Exynos 1330, Exynos 1380, and Exynos 2400 where they do not properly check the length of the data, which can lead to a Information disclosure. **CVE ID: CVE-2024-27362**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27362/	H-SAM-EXYN-230724/3388
Product: exynos_2100					
Affected Version(s): -					
Improper Validation of Specified	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile	https://semiconductor.samsung.com/support/q	H-SAM-EXYN-230724/3389

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Quantity in Input			Processors Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, and Exynos W930 where they do not properly check length of the data, which can lead to a Denial of Service. **CVE ID: CVE-2024-27360**	uality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27360/	
Product: exynos_2200					
Affected Version(s): -					
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, and Exynos W930 where they do not properly check length of the data, which can lead to a Denial of Service. **CVE ID: CVE-2024-27360**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27360/	H-SAM-EXYN-230724/3390
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 1280, Exynos 2200, Exynos 1330, Exynos 1380, and	https://semiconductor.samsung.com/support/quality-support/product-security-updates/,	H-SAM-EXYN-230724/3391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos 2400 where they do not properly check the length of the data, which can lead to a Information disclosure. **CVE ID: CVE-2024-27362**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27362/	
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 2200 and Exynos 2400 where they lack a check for the validation of native handles, which can result in a DoS(Denial of Service) attack by unmapping an invalid length. **CVE ID: CVE-2024-31957**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-31957/	H-SAM-EXYN-230724/3392
Product: exynos_2400					
Affected Version(s): -					
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 1280, Exynos 2200, Exynos 1330, Exynos 1380, and Exynos 2400 where they do not properly check the length of the data, which can lead to a Information disclosure.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27362/	H-SAM-EXYN-230724/3393

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-27362		
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 2200 and Exynos 2400 where they lack a check for the validation of native handles, which can result in a DoS(Denial of Service) attack by unmapping an invalid length. **CVE ID: CVE-2024-31957**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-31957/	H-SAM-EXYN-230724/3394
Product: exynos_850					
Affected Version(s): -					
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, and Exynos W930 where they do not properly check length of the data, which can lead to a Denial of Service. **CVE ID: CVE-2024-27360**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27360/	H-SAM-EXYN-230724/3395
Product: exynos_modem_5300					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jul-2024	3.7	A vulnerability in Samsung Exynos Modem 5300 allows a Man-in-the-Middle (MITM) attacker to downgrade the security mode of packets going to the victim, enabling the attacker to send messages to the victim in plaintext. **CVE ID: CVE-2024-28067**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-28067/	H-SAM-EXYN-230724/3396
Product: exynos_w930					
Affected Version(s): -					
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, and Exynos W930 where they do not properly check length of the data, which can lead to a Denial of Service. **CVE ID: CVE-2024-27360**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27360/	H-SAM-EXYN-230724/3397
Vendor: Schneider-electric					
Product: modicon_lmc058					
Affected Version(s): -					
Improper Neutralization of Input	11-Jul-2024	6.1	CWE-79: Improper Neutralization of Input During Web	https://download.schneider-electric.com/file	H-SCH-MODI-230724/3398

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')			Page Generation ('Cross-site Scripting') vulnerability exists that could cause a vulnerability leading to a cross-site scripting condition where attackers can have a victim's browser run arbitrary JavaScript when they visit a page containing the injected payload. **CVE ID: CVE-2024-6528**	s?p_Doc_Ref=SEVD-2024-191-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-191-04.pdf	
Product: modicon_m241					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2024	6.1	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause a vulnerability leading to a cross-site scripting condition where attackers can have a victim's browser run arbitrary JavaScript when they visit a page containing the injected payload.	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-191-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-191-04.pdf	H-SCH-MODI-230724/3399

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-6528		
Product: modicon_m251					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2024	6.1	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause a vulnerability leading to a cross-site scripting condition where attackers can have a victim's browser run arbitrary JavaScript when they visit a page containing the injected payload. **CVE ID: CVE-2024-6528**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-191-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-191-04.pdf	H-SCH-MODI-230724/3400
Product: modicon_m258					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2024	6.1	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause a vulnerability leading to a cross-site scripting condition where attackers can have	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-191-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-191-04.pdf	H-SCH-MODI-230724/3401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a victim's browser run arbitrary JavaScript when they visit a page containing the injected payload. **CVE ID: CVE-2024-6528**		
Product: modicon_m262					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2024	6.1	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause a vulnerability leading to a cross-site scripting condition where attackers can have a victim's browser run arbitrary JavaScript when they visit a page containing the injected payload. **CVE ID: CVE-2024-6528**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-191-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-191-04.pdf	H-SCH-MODI-230724/3402
Product: whc-5918a					
Affected Version(s): -					
N/A	11-Jul-2024	7.5	CWE-200: Information Exposure vulnerability exists that could cause disclosure of	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-191-01&p_enDocType=Security+an	H-SCH-WHC--230724/3403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			credentials when a specially crafted message is sent to the device. **CVE ID: CVE-2024-6407**	d+Safety+Notice&p_File_Name=SEVD-2024-191-01.pdf	
Vendor: Tenda					
Product: ac8v4					
Affected Version(s): -					
N/A	09-Jul-2024	9.8	Vulnerability in Tenda AC8v4 .V16.03.34.09 due to sscanf and the last digit of s8 being overwritten with \x0. After executing set_client_qos, control over the gp register can be obtained. **CVE ID: CVE-2023-48194**	N/A	H-TEN-AC8V-230724/3404
Operating System					
Vendor: ABB					
Product: aspect-ent-12_firmware					
Affected Version(s): * Up to (including) 3.08.01					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-ASPE-240724/3405

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NEXUS Series: through 3.08.01; MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-ASPE-240724/3406
Product: aspect-ent-256_firmware					
Affected Version(s): * Up to (including) 3.08.01					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series:	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-ASPE-240724/3407

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
			through 3.08.01; MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-ASPE-240724/3408
Product: aspect-ent-2_firmware					
Affected Version(s): * Up to (including) 3.08.01					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-ASPE-240724/3409

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-ASPE-240724/3410
Product: aspect-ent-96_firmware					
Affected Version(s): * Up to (including) 3.08.01					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-ASPE-240724/3411

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
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-ASPE-240724/3412
Product: matrix-11_firmware					
Affected Version(s): * Up to (including) 3.08.01					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-MATR-240724/3413

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-MATR-240724/3414
Product: matrix-216_firmware					
Affected Version(s): * Up to (including) 3.08.01					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-MATR-240724/3415

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
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-MATR-240724/3416
Product: matrix-232_firmware					
Affected Version(s): * Up to (including) 3.08.01					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-MATR-240724/3417

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
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-MATR-240724/3418
Product: matrix-264_firmware					
Affected Version(s): * Up to (including) 3.08.01					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-MATR-240724/3419

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
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-MATR-240724/3420
Product: matrix-296_firmware					
Affected Version(s): * Up to (including) 3.08.01					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-MATR-240724/3421

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-MATR-240724/3422
Product: nexus-2128-a_firmware					
Affected Version(s): * Up to (including) 3.08.01					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3423

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
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3424
Product: nexus-2128-f_firmware					
Affected Version(s): * Up to (including) 3.08.01					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3425

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3426
Product: nexus-2128-g_firmware					
Affected Version(s): * Up to (including) 3.08.01					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3427

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
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3428
Product: nexus-2128_firmware					
Affected Version(s): * Up to (including) 3.08.01					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3429

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
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3430
Product: nexus-264-a_firmware					
Affected Version(s): * Up to (including) 3.08.01					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3431

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3432
Product: nexus-264-f_firmware					
Affected Version(s): * Up to (including) 3.08.01					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3433

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
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3434
Product: nexus-264-g_firmware					
Affected Version(s): * Up to (including) 3.08.01					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3435

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
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3436
Product: nexus-264_firmware					
Affected Version(s): * Up to (including) 3.08.01					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3437

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
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3438
Product: nexus-3-2128_firmware					
Affected Version(s): * Up to (including) 3.08.01					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3439

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3440
Product: nexus-3-264_firmware					
Affected Version(s): * Up to (including) 3.08.01					
N/A	05-Jul-2024	9.8	Improper Input Validation vulnerability in ABB ASPECT-Enterprise on Linux, ABB NEXUS Series on Linux, ABB MATRIX Series on Linux allows Remote Code Inclusion.This issue affects ASPECT-Enterprise: through 3.08.01; NEXUS Series: through 3.08.01;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3441

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
			MATRIX Series: through 3.08.01. **CVE ID: CVE-2024-6298**		
Files or Directories Accessible to External Parties	05-Jul-2024	7.5	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v <=3.08.01; NEXUS Series v <=3.08.01 ; MATRIX Series v<=3.08.01 allows Attacker to access files unauthorized **CVE ID: CVE-2024-6209**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.39956449.23035250.1719878527-141379670.1701144964	O-ABB-NEXU-240724/3442
Vendor: Amazon					
Product: linux_2023					
Affected Version(s): -					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	O-AMA-LINU-240724/3443

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			within a set time period. **CVE ID: CVE-2024-6387**		
Vendor: Apple					
Product: macos					
Affected Version(s): -					
N/A	09-Jul-2024	7	In Docker Desktop before v4.29.0, an attacker who has gained access to the Docker Desktop VM through a container breakout can further escape to the host by passing extensions and dashboard related IPC messages. Docker Desktop v4.29.0 https://docs.docker.com/desktop/release-notes/#4290 fixes the issue on MacOS, Linux and Windows with Hyper-V backend. As exploitation requires "Allow only extensions distributed through the Docker Marketplace" to be disabled, Docker Desktop v4.31.0 https://docs.docker.com/desktop/release-	N/A	O-APP-MACO-240724/3444

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
			notes/#4310 additionally changes the default configuration to enable this setting by default. **CVE ID: CVE-2024-6222**		
Vendor: Canonical					
Product: ubuntu_linux					
Affected Version(s): 22.04					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	O-CAN-UBUN-240724/3445
Affected Version(s): 22.10					
Concurrent Execution using Shared Resource with Improper Synchronization	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/	O-CAN-UBUN-240724/3446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	item?id=40843778	
Affected Version(s): 23.04					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	O-CAN-UBUN-240724/3447
Vendor: Cisco					
Product: nx-os					
Affected Version(s): 10.1\\(1\\)					
Improper Neutralization of Special Elements used in an	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-NX-O-240724/3448

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
OS Command ('OS Command Injection')			arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials.	nxos-cmd-injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-20399		
Affected Version(s): 10.1\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3449

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
			Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 10.2\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3450

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
			attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 10.2\\(1q\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 10.2\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3452

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
			validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 10.2\\(3\\)					
Improper Neutralization of Special Elements used in an OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-	O-CIS-NX-O-240724/3453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**	injection-xD9OhyOP	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): 10.2\\(4\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3454

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 10.2\\(5\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3455

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 10.2\\(6\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 10.2\\(7\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 10.2\\(8\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3458

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
Command Injection')			operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 10.3\\(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
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3459

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 10.3\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3460

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 10.3\\(3\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3461

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 10.3\\(4a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3462

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
			commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 10.3\\(5\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3463

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 10.3\\(99w\\)					
Improper Neutralization of	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could	https://sec.cloudapps.cisco.com/security/cente	O-CIS-NX-O-240724/3464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	r/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 10.3\\(99x\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 10.4\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3466

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
			command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 10.4\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3467

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
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a6\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3468

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a6\\(1a\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a6\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a6\\(2a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3471

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a6\\(3\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3472

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a6\\(3a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3473

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a6\\(4\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a6\\(4a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a6\\(5\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3476

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
			command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a6\\(5a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a6\\(5b\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3478

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
			This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a6\\(6\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a6\\(7\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3480

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a6\\(8\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3481

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a8\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3482

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a8\\(10\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3483

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a8\\(10a\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a8\\(11\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3485

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a8\\(11a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3486

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a8\\(11b\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a8\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3488

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a8\\(3\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a8\\(4\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3490

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a8\\(4a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3491

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
			command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a8\\(5\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3492

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a8\\(6\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3493

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
			This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a8\\(7\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a8\\(7a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3495

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
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a8\\(7b\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3496

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a8\\(8\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3497

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
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)a8\\(9\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3498

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)u6\\(1\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)u6\\(10\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)u6\\(1a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3501

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)u6\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)u6\\(2a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3503

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)u6\\(3\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)u6\\(3a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)u6\\(4\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3506

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
			command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)u6\\(4a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3507

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)u6\\(5\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3508

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
			This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)u6\\(5a\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)u6\\(5b\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)u6\\(5c\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3511

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)u6\\(6\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3512

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)u6\\(7\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3513

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
			This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)u6\\(8\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.0\\(2\\)u6\\(9\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3516

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(10\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3517

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(11\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3518

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(11b\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3519

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
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(11c\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3520

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(11d\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3521

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(11e\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3522

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(12\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3523

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(13\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(13a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3525

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(13b\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3526

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(14\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(15\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3528

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(16\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(17\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3530

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
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(18\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3531

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(19\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3533

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(20\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(20a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(21\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3536

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(22\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3537

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(23\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3538

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(24\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(24a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3540

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(25\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3541

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
			command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(27\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(29\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3543

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(2a\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(3\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3545

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(31\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3546

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(33\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3547

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
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(5\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3548

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(5a\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3549

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(5b\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3550

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(6\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3551

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(6a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3552

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
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(6b\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3553

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(7\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(8\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3555

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(8a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3556

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(8b\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3557

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(9\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3558

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
			This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(9a\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(9b\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3560

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 6.2\\(9c\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3561

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)f1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3562

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)f2\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3563

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)f2\\(2\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)f3\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3565

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)f3\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3566

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)f3\\(3\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3567

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)f3\\(3a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3568

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)f3\\(3c\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)f3\\(4\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3570

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)f3\\(5\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3571

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i4\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3572

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i4\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3573

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i4\\(3\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i4\\(4\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i4\\(5\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3576

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i4\\(6\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3577

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i4\\(7\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3578

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i4\\(8\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i4\\(8a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i4\\(8b\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3581

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i4\\(8z\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3582

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i4\\(9\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3583

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i5\\(1\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i5\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3585

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i6\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3586

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
			command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i6\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3587

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i7\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3588

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i7\\(10\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i7\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i7\\(3\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3591

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i7\\(4\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3592

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i7\\(5\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3593

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i7\\(5a\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i7\\(6\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i7\\(7\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3596

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i7\\(8\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3597

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
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.0\\(3\\)i7\\(9\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3598

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.1\\(0\\)n1\\(1\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.1\\(0\\)n1\\(1a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.1\\(0\\)n1\\(1b\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3601

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.1\\(1\\)n1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3602

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.1\\(2\\)n1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3603

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.1\\(3\\)n1\\(1\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.1\\(3\\)n1\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3605

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.1\\(4\\)n1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3606

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.1\\(5\\)n1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.1\\(5\\)n1\\(1b\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3608

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
			This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.2\\(0\\)d1\\(1\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.2\\(1\\)d1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3610

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.2\\(2\\)d1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3611

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.2\\(2\\)d1\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3612

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(0\\)d1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3613

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(0\\)dx\\(1\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(0\\)dy\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(0\\)n1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3616

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(1\\)d1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3617

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(1\\)dy\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3618

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(1\\)n1\\(1\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(10\\)n1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(11\\)n1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3621

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(12\\)n1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3622

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(13\\)n1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3623

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(14\\)n1\\(1\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(2\\)d1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3625

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
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(2\\)d1\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3626

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(2\\)d1\\(3\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3627

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(2\\)d1\\(3a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3628

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(2\\)n1\\(1\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(3\\)d1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3630

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(3\\)n1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3631

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
			command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(4\\)d1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(4\\)n1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3633

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(5\\)d1\\(1\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(5\\)n1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(6\\)d1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3636

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(6\\)n1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3637

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
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(7\\)d1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3638

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(7\\)n1\\(1\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(7\\)n1\\(1a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(7\\)n1\\(1b\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3641

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(8\\)d1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(8\\)n1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3643

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(9\\)d1\\(1\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 7.3\\(9\\)n1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3645

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.0\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3646

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.1\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.1\\(1a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3648

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.1\\(1b\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.1\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3650

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.1\\(2a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3651

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.2\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.2\\(10\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3653

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.2\\(11\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.2\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.2\\(3\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3656

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.2\\(4\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3657

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.2\\(5\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3658

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.2\\(6\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.2\\(7\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.2\\(7a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3661

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.2\\(8\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3662

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.2\\(9\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3663

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.3\\(1\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.3\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3665

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.4\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3666

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.4\\(1a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3667

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
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.4\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3668

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
			This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.4\\(2a\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.4\\(2b\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3670

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
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.4\\(2c\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3671

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
			command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.4\\(2d\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3672

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
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.4\\(2e\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3673

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.4\\(2f\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.4\\(3\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3675

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
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.4\\(4\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3676

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.4\\(4a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3677

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.4\\(5\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3678

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
			This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.4\\(6\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.4\\(6a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3680

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.4\\(7\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3681

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
			command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.4\\(8\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3682

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.4\\(9\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3683

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 8.5\\(1\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.2\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.2\\(1a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3686

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.2\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3687

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
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.2\\(2t\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3688

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.2\\(2v\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3689

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.2\\(3\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.2\\(4\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3691

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.3\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3692

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.3\\(10\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3693

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
			This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.3\\(11\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.3\\(12\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3695

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.3\\(13\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3696

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
			command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.3\\(2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3697

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.3\\(2a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3698

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
			This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.3\\(3\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.3\\(4\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3700

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.3\\(5\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3701

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.3\\(6\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3702

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
			attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.3\\(7\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3703

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.3\\(7a\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.3\\(8\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3705

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
			with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.3\\(9\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3706

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.4\\(1\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3707

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.4\\(1a\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	O-CIS-NX-O-240724/3708

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
			This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. **CVE ID: CVE-2024-20399**		
Affected Version(s): 9.4\\(2\\)					
Improper Neutralization of Special	01-Jul-2024	6.7	A vulnerability in the CLI of Cisco NX-OS Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-240724/3709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have	SecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator credentials. **CVE ID: CVE-2024-20399**		
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 12.0					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	O-DEB-DEBI-240724/3710
Vendor: Dlink					
Product: dar-7000_firmware					
Affected Version(s): * Up to (including) 2023-09-22					
Deserialization of Untrusted Data	05-Jul-2024	8.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DAR-7000 up to 20230922. It has been rated as problematic. Affected by this issue is some	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10354	O-DLI-DAR--240724/3711

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
			unknown functionality of the file /log/decodmail.php. The manipulation of the argument file leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-270368. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID: CVE-2024-6525**		
Product: dir-823x_ax3000_firmware					
Affected Version(s): 240126					
N/A	08-Jul-2024	8.8	D-Link DIR-823X firmware - 240126 was discovered to contain a remote command execution (RCE) vulnerability via the dhcpd_startip parameter at /goform/set_lan_settings. **CVE ID: CVE-2024-39202**	N/A	O-DLI-DIR--240724/3712
Vendor: Freebsd					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: freebsd					
Affected Version(s): 13.2					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	O-FRE-FREE-240724/3713
Affected Version(s): 13.3					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	O-FRE-FREE-240724/3714

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
			CVE ID: CVE-2024-6387		
Affected Version(s): 14.0					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	O-FRE-FREE-240724/3715
Affected Version(s): 14.1					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	O-FRE-FREE-240724/3716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-6387		
Vendor: Google					
Product: android					
Affected Version(s): 14.0					
N/A	02-Jul-2024	3.3	Improper input validation in Tips prior to version 6.2.9.4 in Android 14 allows local attacker to send broadcast with Tips' privilege. **CVE ID: CVE-2024-34599**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=07	O-GOO-ANDR-240724/3717
Vendor: kiloview					
Product: p1_firmware					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-2024	5.4	A 'Cross-site Scripting' (XSS) vulnerability, characterized by improper input neutralization during web page generation, has been discovered. This vulnerability allows for Stored XSS attacks to occur. Multiple areas within the administration interface of the webserver lack adequate input validation, resulting in multiple instances	N/A	O-KIL-P1_F-240724/3718

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Stored XSS vulnerabilities. **CVE ID: CVE-2023-41922**		
Product: p2_firmware					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-2024	5.4	A 'Cross-site Scripting' (XSS) vulnerability, characterized by improper input neutralization during web page generation, has been discovered. This vulnerability allows for Stored XSS attacks to occur. Multiple areas within the administration interface of the webserver lack adequate input validation, resulting in multiple instances of Stored XSS vulnerabilities. **CVE ID: CVE-2023-41922**	N/A	O-KIL-P2_F-240724/3719
Vendor: level1					
Product: wbr-6013_firmware					
Affected Version(s): rer4_a_v3411b_2t2r_lev_09_170623					
Use of Hard-coded Credentials	08-Jul-2024	9.8	A hard-coded password vulnerability exists in the telnetd functionality of LevelOne WBR-6013	N/A	O-LEV-WBR--240724/3720

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
			RER4_A_v3411b_2T2R_LEV_09_170623. A set of specially crafted network packets can lead to arbitrary command execution. **CVE ID: CVE-2023-46685**		
Cross-Site Request Forgery (CSRF)	08-Jul-2024	8.8	A cross-site request forgery (csrf) vulnerability exists in the boa CSRF protection functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted network request can lead to CSRF. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID: CVE-2023-47677**	N/A	O-LEV-WBR--240724/3721
Improper Verification of Cryptographic Signature	08-Jul-2024	7.2	A firmware update vulnerability exists in the boa formUpload functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted network packets can lead to arbitrary firmware update. An attacker can provide a malicious file to	N/A	O-LEV-WBR--240724/3722

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 this vulnerability. **CVE ID: CVE-2023-34435**		
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa formRoute functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID: CVE-2023-41251**	N/A	O-LEV-WBR--240724/3723
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa setRepeaterSsid functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID: CVE-2023-45215**	N/A	O-LEV-WBR--240724/3724

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	08-Jul-2024	7.2	An integer overflow vulnerability exists in the boa updateConfigIntoFlash functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID: CVE-2023-45742**	N/A	O-LEV-WBR--240724/3725
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa set_RadvdPrefixParam functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID: CVE-2023-47856**	N/A	O-LEV-WBR--240724/3726
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa formDnsv6 functionality of	N/A	O-LEV-WBR--240724/3727

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID: CVE-2023-48270**		
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa formFilter functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID: CVE-2023-49073**	N/A	O-LEV-WBR--240724/3728
N/A	08-Jul-2024	7.2	Leftover debug code exists in the boa formSysCmd functionality of LevelOne WBR-6013 RER4_A_v3411b_2T2R_LEV_09_170623. A specially crafted network request can lead to	N/A	O-LEV-WBR--240724/3729

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
			arbitrary command execution. **CVE ID: CVE-2023-49593**		
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa rollback_control_code functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID: CVE-2023-49595**	N/A	O-LEV-WBR--240724/3730
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send a series of HTTP requests to trigger this vulnerability. **CVE ID: CVE-2023-49867**	N/A	O-LEV-WBR--240724/3731

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	08-Jul-2024	7.2	Two stack-based buffer overflow vulnerabilities exist in the boa set_RadvdInterface Param functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `interfacename` request's parameter. **CVE ID: CVE-2023-50239**	N/A	O-LEV-WBR--240724/3732
Out-of-bounds Write	08-Jul-2024	7.2	Two stack-based buffer overflow vulnerabilities exist in the boa set_RadvdInterface Param functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to remote code execution. An attacker can send a sequence of	N/A	O-LEV-WBR--240724/3733

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `AdvDefaultPreference` request's parameter. **CVE ID: CVE-2023-50240**		
Out-of-bounds Write	08-Jul-2024	7.2	Two stack-based buffer overflow vulnerabilities exist in the boa formIpQoS functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `comment` request's parameter. **CVE ID: CVE-2023-50243**	N/A	O-LEV-WBR--240724/3734
Out-of-bounds Write	08-Jul-2024	7.2	Two stack-based buffer overflow vulnerabilities exist in the boa formIpQoS functionality of Realtek rtl819x	N/A	O-LEV-WBR--240724/3735

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
			Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `entry_name` request's parameter. **CVE ID: CVE-2023-50244**		
Out-of-bounds Write	08-Jul-2024	7.2	A stack-based buffer overflow vulnerability exists in the boa getInfo functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send a series of HTTP requests to trigger this vulnerability. **CVE ID: CVE-2023-50330**	N/A	O-LEV-WBR--240724/3736
Improper Neutralization of Special Elements used in an OS	08-Jul-2024	7.2	Three os command injection vulnerabilities exist in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11.	N/A	O-LEV-WBR--240724/3737

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 ('OS Command Injection')			A specially crafted series of HTTP requests can lead to arbitrary command execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This command injection is related to the `targetAPSsid` request's parameter. **CVE ID: CVE-2023-50381**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jul-2024	7.2	Three os command injection vulnerabilities exist in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary command execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This command injection is related to the `peerPin` request's parameter. **CVE ID: CVE-2023-50382**	N/A	O-LEV-WBR--240724/3738
Improper Neutralization of	08-Jul-2024	7.2	Three os command injection vulnerabilities exist	N/A	O-LEV-WBR--240724/3739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary command execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This command injection is related to the `localPin` request's parameter. **CVE ID: CVE-2023-50383**		
Out-of-bounds Write	08-Jul-2024	7.2	A heap-based buffer overflow vulnerability exists in the configuration file mib_init_value_array functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted .dat file can lead to arbitrary code execution. An attacker can upload a malicious file to trigger this vulnerability. **CVE ID: CVE-2024-21778**	N/A	O-LEV-WBR--240724/3740
Vendor: Linux					
Product: linux_kernel					
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
N/A	09-Jul-2024	7	In Docker Desktop before v4.29.0, an attacker who has gained access to the Docker Desktop VM through a container breakout can further escape to the host by passing extensions and dashboard related IPC messages. Docker Desktop v4.29.0 https://docs.docker.com/desktop/release-notes/#4290 fixes the issue on MacOS, Linux and Windows with Hyper-V backend. As exploitation requires "Allow only extensions distributed through the Docker Marketplace" to be disabled, Docker Desktop v4.31.0 https://docs.docker.com/desktop/release-notes/#4310 additionally changes the default configuration to enable this setting by default. **CVE ID: CVE-2024-6222**	N/A	O-LIN-LINU-240724/3741

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
Affected Version(s): * Up to (excluding) 2.6.33					
Allocation of Resources Without Limits or Throttling	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mmc: davinci: Don't strip remove function when driver is builtin Using __exit for the remove function results in the remove callback being discarded with CONFIG_MMC_DAVINCI=y. When such a device gets unbound (e.g. using sysfs or hotplug), the driver is just removed without the cleanup being performed. This results in resource leaks. Fix it by compiling in the remove callback unconditionally. This also fixes a W=1 modpost warning: WARNING: modpost:	https://git.kernel.org/stable/c/1d5ed0efe51d36b9ae9b64f133bf41cdbf56f584, https://git.kernel.org/stable/c/55c421b364482b61c4c45313a535e61ed5ae4ea3, https://git.kernel.org/stable/c/5ee241f72edc6dce5051a5f100eab6cc019d873e	O-LIN-LINU-240724/3742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drivers/mmc/host /davinci_mmc: section mismatch in reference: davinci_mmcsd_driver+0x10 (section: .data) -> davinci_mmcsd_remove (section: .exit.text) **CVE ID: CVE-2024-39484**		
Affected Version(s): * Up to (excluding) 5.17					
Allocation of Resources Without Limits or Throttling	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/vmalloc: fix vmalloc which may return null if called with __GFP_NOFAIL commit a421ef303008 ("mm: allow !GFP_KERNEL allocations for kvmalloc") includes support for __GFP_NOFAIL, but it presents a conflict with commit dd544141b9eb ("vmalloc: back off when the current task is OOM-killed"). A	https://git.kernel.org/stable/c/198a80833e3421d4c9820a4ae907120adf598c91, https://git.kernel.org/stable/c/758678b65164b2158fc1de411092191cb3c394d4, https://git.kernel.org/stable/c/8e0545c83d672750632f46e3f9ad95c48c91a0fc	O-LIN-LINU-240724/3743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible scenario is as follows: process-a __vmalloc_node_range(GFP_KERNEL | __GFP_NOFAIL) __vmalloc_area_node() vm_area_alloc_pages() --> oom-killer send SIGKILL to process-a if (fatal_signal_pending(current)) break; --> return NULL; To fix this, do not check fatal_signal_pending() in vm_area_alloc_pages() if __GFP_NOFAIL set. This issue occurred during OPLUS KASAN TEST. Below is part of the log -> oom-killer sends signal to process		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[65731.222840] [T1308] oom-kill:constraint=CONSTRAINT_NONE,nodemask=(null),cpuset=/,mems_allowed=0,global_oom,task_memcg=/apps/uid_10198,task=gs.intelligence,pid=32454,uid=10198 [65731.259685] [T32454] Call trace: [65731.259698] [T32454] dump_backtrace+0xf4/0x118 [65731.259734] [T32454] show_stack+0x18/0x24 [65731.259756] [T32454] dump_stack_lvl+0x60/0x7c [65731.259781] [T32454] dump_stack+0x18/0x38 [65731.259800] [T32454] mrdump_common_die+0x250/0x39c [mrdump] [65731.259936] [T32454] ipanic_die+0x20/0x34 [mrdump]		

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[65731.260019] [T32454] atomic_notifier_call_chain+0xb4/0xfc [65731.260047] [T32454] notify_die+0x114/0x198 [65731.260073] [T32454] die+0xf4/0x5b4 [65731.260098] [T32454] die_kernel_fault+0x80/0x98 [65731.260124] [T32454] __do_kernel_fault+0x160/0x2a8 [65731.260146] [T32454] do_bad_area+0x68/0x148 [65731.260174] [T32454] do_mem_abort+0x151c/0x1b34 [65731.260204] [T32454] el1_abort+0x3c/0x5c [65731.260227] [T32454] el1h_64_sync_handler+0x54/0x90 [65731.260248] [T32454] el1h_64_sync+0x68/0x6c		

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[65731.260269] [T32454] z_erofs_decompress_queue+0x7f0/0x2258 --> be->decompressed_pages = kvcalloc(be->nr_pages, sizeof(struct page *), GFP_KERNEL | __GFP_NOFAIL); kernel panic by NULL pointer dereference. erofs assume kvmalloc with __GFP_NOFAIL never return NULL. [65731.260293] [T32454] z_erofs_runqueue+0xf30/0x104c [65731.260314] [T32454] z_erofs_readahead+0x4f0/0x968 [65731.260339] [T32454] read_pages+0x170/0xadc [65731.260364] [T32454] page_cache_ra_unbounded+0x874/0xf30 [65731.260388] [T32454] page_cache_ra_order+0x24c/0x714		

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[65731.260411] [T32454] filemap_fault+0xbf0/0x1a74 [65731.260437] [T32454] __do_fault+0xd0/0x33c [65731.260462] [T32454] handle_mm_fault+0xf74/0x3fe0 [65731.260486] [T32454] do_mem_abort+0x54c/0x1b34 [65731.260509] [T32454] el0_da+0x44/0x94 [65731.260531] [T32454] el0t_64_sync_handler+0x98/0xb4 [65731.260553] [T32454] el0t_64_sync+0x198/0x19c **CVE ID: CVE-2024-39474**		
Affected Version(s): * Up to (excluding) 6.3					
N/A	05-Jul-2024	7.5	The IPv6 implementation in the Linux kernel before 6.3 has a net/ipv6/route.c max_size threshold that can be consumed easily, e.g., leading to a denial of service (network is	https://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.3, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id=af6d10345ca76670c1b7c3779	O-LIN-LINU-240724/3744

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
			unreachable errors) when IPv6 packets are sent in a loop via a raw socket. **CVE ID: CVE-2023-52340**	9f0d5576ccef277	
Affected Version(s): * Up to (excluding) 6.4					
NULL Pointer Dereference	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: ipc4-topology: Fix input format query of process modules without base extension If a process module does not have base config extension then the same format applies to all of it's inputs and the process->base_config_ext is NULL, causing NULL dereference when specifically crafted topology and sequences used. **CVE ID: CVE-2024-39473**	https://git.kernel.org/stable/c/9e16f17a2a0e97b43538b272e7071537a3e03368, https://git.kernel.org/stable/c/e3ae00ee238bce6cfa5ad935c921181c14d18fd6, https://git.kernel.org/stable/c/ffa077b2f6ad124ec3d23fbddc5e4b0ff2647af8	O-LIN-LINU-240724/3745
N/A	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/1d87cf2eba46deaff614236612	O-LIN-LINU-240724/3746

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			KVM: SVM: WARN on vNMI + NMI window iff NMIs are outright masked When requesting an NMI window, WARN on vNMI support being enabled if and only if NMIs are actually masked, i.e. if the vCPU is already handling an NMI. KVM's ABI for NMIs that arrive simultanesouly (from KVM's point of view) is to inject one NMI and pend the other. When using vNMI, KVM pends the second NMI simply by setting V_NMI_PENDING, and lets the CPU do the rest (hardware automatically sets V_NMI_BLOCKING when an NMI is injected). However, if KVM can't immediately	7f2323de9f84d1, https://git.kernel.org/stable/c/b4bd556467477420ee3a91fbcba73c579669edc6, https://git.kernel.org/stable/c/f79edaf7370986d73d204b36c50cc563a4c0f356	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject an NMI, e.g. because the vCPU is in an STI shadow or is running with GIF=0, then KVM will request an NMI window and trigger the WARN (but still function correctly). Whether or not the GIF=0 case makes sense is debatable, as the intent of KVM's behavior is to provide functionality that is as close to real hardware as possible. E.g. if two NMIs are sent in quick succession, the probability of both NMIs arriving in an STI shadow is infinitesimally low on real hardware, but significantly larger in a virtual environment, e.g. if the vCPU is preempted in the STI shadow. For GIF=0, the argument isn't as clear cut, because the window where two		

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NMIs can collide is much larger in bare metal (though still small). That said, KVM should not have divergent behavior for the GIF=0 case based on whether or not vNMI support is enabled. And KVM has allowed simultaneous NMIs with GIF=0 for over a decade, since commit 7460fb4a3400 ("KVM: Fix simultaneous NMIs"). I.e. KVM's GIF=0 handling shouldn't be modified without a *really* good reason to do so, and if KVM's behavior were to be modified, it should be done irrespective of vNMI support. **CVE ID: CVE-2024-39483**		
Affected Version(s): * Up to (excluding) 6.6.34					
Improper Initialization	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/1aa6cd4adfc0380fa1ccc2f1468	O-LIN-LINU-240724/3747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			media: v4l: async: Properly re-initialise notifier entry in unregister The notifier_entry of a notifier is not re-initialised after unregistering the notifier. This leads to dangling pointers being left there so use list_del_init() to return the notifier_entry an empty list. **CVE ID: CVE-2024-39485**	48940ff882a66, https://git.kernel.org/stable/c/87100b09246202a91fce4a1562955c32229173bb, https://git.kernel.org/stable/c/9537a8425a7a0222999d5839a0b394b1e8834b4a	
Affected Version(s): * Up to (including) 6.9.3					
Allocation of Resources Without Limits or Throttling	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: xfs: fix log recovery buffer allocation for the legacy h_size fixup Commit a70f9fe52daa ("xfs: detect and handle invalid iclog size set by mkfs") added a fixup for incorrect	https://git.kernel.org/stable/c/45cf976008ddef4a9c9a30310c9b4fb2a9a6602a	O-LIN-LINU-240724/3748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			h_size values used for the initial umount record in old xfsprogs versions. Later commit 0c771b99d6c9 ("xfs: clean up calculation of LR header blocks") cleaned up the log reover buffer calculation, but stoped using the fixed up h_size value to size the log recovery buffer, which can lead to an out of bounds access when the incorrect h_size does not come from the old mkfs tool, but a fuzzer. Fix this by open coding xlog_logrec_hblks and taking the fixed h_size into account for this calculation. **CVE ID: CVE-2024-39472**		
Affected Version(s): 6.10.0					
NULL Pointer Dereference	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/9e16f17a2a0e97b43538b272e	O-LIN-LINU-240724/3749

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ASoC: SOF: ipc4-topology: Fix input format query of process modules without base extension If a process module does not have base config extension then the same format applies to all of it's inputs and the process->base_config_ext is NULL, causing NULL dereference when specifically crafted topology and sequences used. **CVE ID: CVE-2024-39473**	7071537a3e03368, https://git.kernel.org/stable/c/e3ae00ee238bce6cfa5ad935c921181c14d18fd6, https://git.kernel.org/stable/c/ffa077b2f6ad124ec3d23fbddc5e4b0ff2647af8	
Allocation of Resources Without Limits or Throttling	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/hugetlb: do not call vma_add_reservation upon ENOMEM sysbot reported a splat [1] on __unmap_hugepage_range(). This is because	https://git.kernel.org/stable/c/8daf9c702ee7f825f0de8600abff764acfedea13, https://git.kernel.org/stable/c/aa998f9dcb34c28448f86e8f5490f20d5eb0eac7	O-LIN-LINU-240724/3750

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
			vma_needs_reservation() can return -ENOMEM if allocate_file_region_entries() fails to allocate the file_region struct for the reservation. Check for that and do not call vma_add_reservation() if that is the case, otherwise region_abort() and region_del() will see that we do not have any file_regions. If we detect that vma_needs_reservation() returned -ENOMEM, we clear the hugetlb_restore_reserve flag as if this reservation was still consumed, so free_huge_folio() will not increment the resv count. [1] https://lore.kernel.org/linux-mm/000000000004096100617c58d54@google.com/T/		

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			#ma5983bc1ab18a54910da83416b3f89f3c7ee43aa **CVE ID: CVE-2024-39477**		
N/A	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: KVM: SVM: WARN on vNMI + NMI window iff NMIs are outright masked When requesting an NMI window, WARN on vNMI support being enabled if and only if NMIs are actually masked, i.e. if the vCPU is already handling an NMI. KVM's ABI for NMIs that arrive simultanesouly (from KVM's point of view) is to inject one NMI and pend the other. When using vNMI, KVM pends the second NMI simply by setting V_NMI_PENDING, and lets the CPU do the	https://git.kernel.org/stable/c/1d87cf2eba46deaff6142366127f2323de9f84d1, https://git.kernel.org/stable/c/b4bd556467477420ee3a91fbcba73c579669edc6, https://git.kernel.org/stable/c/f79edaf7370986d73d204b36c50cc563a4c0f356	O-LIN-LINU-240724/3751

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 (hardware automatically sets V_NMI_BLOCKING when an NMI is injected). However, if KVM can't immediately inject an NMI, e.g. because the vCPU is in an STI shadow or is running with GIF=0, then KVM will request an NMI window and trigger the WARN (but still function correctly). Whether or not the GIF=0 case makes sense is debatable, as the intent of KVM's behavior is to provide functionality that is as close to real hardware as possible. E.g. if two NMIs are sent in quick succession, the probability of both NMIs arriving in an STI shadow is infinitesimally low on real hardware, but significantly larger in a virtual environment, e.g.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			if the vCPU is preempted in the STI shadow. For GIF=0, the argument isn't as clear cut, because the window where two NMIs can collide is much larger in bare metal (though still small). That said, KVM should not have divergent behavior for the GIF=0 case based on whether or not vNMI support is enabled. And KVM has allowed simultaneous NMIs with GIF=0 for over a decade, since commit 7460fb4a3400 ("KVM: Fix simultaneous NMIs"). I.e. KVM's GIF=0 handling shouldn't be modified without a *really* good reason to do so, and if KVM's behavior were to be modified, it should be done irrespective of vNMI support.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-39483		
Improper Initialization	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: media: v4l: async: Properly re-initialise notifier entry in unregister The notifier_entry of a notifier is not re-initialised after unregistering the notifier. This leads to dangling pointers being left there so use list_del_init() to return the notifier_entry an empty list. **CVE ID: CVE-2024-39485**	https://git.kernel.org/stable/c/1aa6cd4adfc0380fa1ccc2f146848940ff882a66, https://git.kernel.org/stable/c/87100b09246202a91fce4a1562955c32229173bb, https://git.kernel.org/stable/c/9537a8425a7a0222999d5839a0b394b1e8834b4a	O-LIN-LINU-240724/3752
Affected Version(s): From (including) 4.19 Up to (excluding) 4.19.316					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: kdb: Fix buffer overflow during tab-complete Currently, when the user attempts symbol completion	https://git.kernel.org/stable/c/107e825cc448b7834b31e8b1b3cf0f57426d46d5, https://git.kernel.org/stable/c/33d9c814652b971461d1e30bead6792851c209e7, https://git.kernel.org/stable/c/	O-LIN-LINU-240724/3753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the Tab key, kdb will use strncpy() to insert the completed symbol into the command buffer. Unfortunately it passes the size of the source buffer rather than the destination to strncpy() with predictably horrible results. Most obviously if the command buffer is already full but cp, the cursor position, is in the middle of the buffer, then we will write past the end of the supplied buffer. Fix this by replacing the dubious strncpy() calls with memmove()/memcpy() calls plus explicit boundary checks to make sure we have enough space before we start moving characters around.	cfdc2fa4db57503bc6d3817240547c8ddc55fa96	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-39480		
Divide By Zero	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fbdev: savage: Handle err return when savagefb_check_var failed The commit 04e5eac8f3ab("fbdev: savage: Error out if pixclock equals zero") checks the value of pixclock to avoid divide-by-zero error. However the function savagefb_probe doesn't handle the error return of savagefb_check_var. When pixclock is 0, it will cause divide-by-zero error. **CVE ID: CVE-2024-39475**	https://git.kernel.org/stable/c/32f92b0078ebf79dbe4827288e0acb50d89d3d5b, https://git.kernel.org/stable/c/4b2c67e30b4e1d2ae19dba8b8e8f3b5fd3cf8089, https://git.kernel.org/stable/c/5f446859bfa46df0ffb34149499f48a2c2d8cd95	O-LIN-LINU-240724/3754
Improper Locking	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: md/raid5: fix deadlock that raid5d() wait for	https://git.kernel.org/stable/c/098d54934814dd876963abfe751c3b1cf7fbe56a, https://git.kernel.org/stable/c/151f66bb618d1	O-LIN-LINU-240724/3755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			itself to clear MD_SB_CHANGE_PENDING Xiao reported that lvm2 test lvconvert-raid-takeover.sh can hang with small possibility, the root cause is exactly the same as commit bed9e27baf52 ("Revert "md/raid5: Wait for MD_SB_CHANGE_PENDING in raid5d"") However, Dan reported another hang after that, and junxiao investigated the problem and found out that this is caused by plugged bio can't issue from raid5d(). Current implementation in raid5d() has a weird dependence: 1) md_check_recovery	fd0eeb84acb61b4a9fa5d8bb0fa, https://git.kernel.org/stable/c/3f8d5e802d4cedd445f9a89be8c3fd2d0e99024b	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 raid5d() must hold 'reconfig_mutex' to clear MD_SB_CHANGE_PENDING; 2) raid5d() handles IO in a deadloop, until all IO are issued; 3) IO from raid5d() must wait for MD_SB_CHANGE_PENDING to be cleared; This behaviour is introduce before v2.6, and for consequence, if other context hold 'reconfig_mutex', and md_check_recovery() can't update super_block, then raid5d() will waste one cpu 100% by the deadloop, until 'reconfig_mutex' is released. Refer to the implementation from raid1 and raid10, fix this problem by		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			skipping issue IO if MD_SB_CHANGE_PENDING is still set after md_check_recovery(), daemon thread will be woken up when 'reconfig_mutex' is released. Meanwhile, the hang problem will be fixed as well. **CVE ID: CVE-2024-39476**		
Affected Version(s): From (including) 5.10 Up to (excluding) 5.10.219					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: kdb: Fix buffer overflow during tab-complete Currently, when the user attempts symbol completion with the Tab key, kdb will use strncpy() to insert the completed symbol into the command buffer. Unfortunately it passes the size of the source buffer rather than the	https://git.kernel.org/stable/c/107e825cc448b7834b31e8b1b3cf0f57426d46d5, https://git.kernel.org/stable/c/33d9c814652b971461d1e30bead6792851c209e7, https://git.kernel.org/stable/c/cfdc2fa4db57503bc6d3817240547c8ddc55fa96	O-LIN-LINU-240724/3756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			destination to strncpy() with predictably horrible results. Most obviously if the command buffer is already full but cp, the cursor position, is in the middle of the buffer, then we will write past the end of the supplied buffer. Fix this by replacing the dubious strncpy() calls with memmove()/memcpy() calls plus explicit boundary checks to make sure we have enough space before we start moving characters around. **CVE ID: CVE-2024-39480**		
Divide By Zero	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fbdev: savage: Handle err return when	https://git.kernel.org/stable/c/32f92b0078ebf79dbe4827288e0acb50d89d3d5b, https://git.kernel.org/stable/c/4b2c67e30b4e1d2ae19dba8b8e	O-LIN-LINU-240724/3757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			savagefb_check_var failed The commit 04e5eac8f3ab("fbdev: savage: Error out if pixclock equals zero") checks the value of pixclock to avoid divide-by-zero error. However the function savagefb_probe doesn't handle the error return of savagefb_check_var. When pixclock is 0, it will cause divide-by-zero error. **CVE ID: CVE-2024-39475**	8f3b5fd3cf8089, https://git.kernel.org/stable/c/5f446859bfa46df0ffb34149499f48a2c2d8cd95	
Improper Locking	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: md/raid5: fix deadlock that raid5d() wait for itself to clear MD_SB_CHANGE_PENDING Xiao reported that lvm2 test lvconvert-raid-takeover.sh can hang with	https://git.kernel.org/stable/c/098d54934814dd876963abfe751c3b1cf7fbe56a, https://git.kernel.org/stable/c/151f66bb618d1fd0eeb84acb61b4a9fa5d8bb0fa, https://git.kernel.org/stable/c/3f8d5e802d4cedd445f9a89be8c3fd2d0e99024b	O-LIN-LINU-240724/3758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			small possibility, the root cause is exactly the same as commit bed9e27baf52 ("Revert "md/raid5: Wait for MD_SB_CHANGE_PENDING in raid5d"") However, Dan reported another hang after that, and junxiao investigated the problem and found out that this is caused by plugged bio can't issue from raid5d(). Current implementation in raid5d() has a weird dependence: 1) md_check_recovery() from raid5d() must hold 'reconfig_mutex' to clear MD_SB_CHANGE_PENDING; 2) raid5d() handles IO in a deadloop,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			until all IO are issued; 3) IO from raid5d() must wait for MD_SB_CHANGE_PENDING to be cleared; This behaviour is introduce before v2.6, and for consequence, if other context hold 'reconfig_mutex', and md_check_recovery() can't update super_block, then raid5d() will waste one cpu 100% by the deadloop, until 'reconfig_mutex' is released. Refer to the implementation from raid1 and raid10, fix this problem by skipping issue IO if MD_SB_CHANGE_PENDING is still set after md_check_recovery(), daemon thread will be woken up when 'reconfig_mutex'		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. Meanwhile, the hang problem will be fixed as well. **CVE ID: CVE-2024-39476**		
Affected Version(s): From (including) 5.10 Up to (excluding) 5.10.221					
Allocation of Resources Without Limits or Throttling	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bcache: fix variable length array abuse in btree_iter btree_iter is used in two ways: either allocated on the stack with a fixed size MAX_BSETS, or from a mempool with a dynamic size based on the specific cache set. Previously, the struct had a fixed-length array of size MAX_BSETS which was indexed out-of-bounds for the dynamically-sized iterators, which causes UBSAN to complain. This patch uses the same approach as	https://git.kernel.org/stable/c/0c31344e22dd8d6b1394c6e4c41d639015bdc671, https://git.kernel.org/stable/c/2c3d7b03b658dc8bfa6112b194b67b92a87e081b, https://git.kernel.org/stable/c/3a861560ccb35f2a4f0a4b8207fa7c2a35fc7f31	O-LIN-LINU-240724/3759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in bcachefs's sort_iter and splits the iterator into a btree_iter with a flexible array member and a btree_iter_stack which embeds a btree_iter as well as a fixed-length data array. **CVE ID: CVE-2024-39482**		
Allocation of Resources Without Limits or Throttling	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mmc: davinci: Don't strip remove function when driver is builtin Using __exit for the remove function results in the remove callback being discarded with CONFIG_MMC_DAVINCI=y. When such a device gets unbound (e.g. using sysfs or hotplug), the driver is just removed without the cleanup being performed. This results in	https://git.kernel.org/stable/c/1d5ed0efe51d36b9ae9b64f133bf41cdbf56f584, https://git.kernel.org/stable/c/55c421b364482b61c4c45313a535e61ed5ae4ea3, https://git.kernel.org/stable/c/5ee241f72edc6dce5051a5f100eab6cc019d873e	O-LIN-LINU-240724/3760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resource leaks. Fix it by compiling in the remove callback unconditionally. This also fixes a W=1 modpost warning: WARNING: modpost: drivers/mmc/host /davinci_mmc: section mismatch in reference: davinci_mmcsd_dri ver+0x10 (section: .data) -> davinci_mmcsd_re move (section: .exit.text) **CVE ID: CVE-2024-39484**		
Affected Version(s): From (including) 5.15 Up to (excluding) 5.15.161					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: kdb: Fix buffer overflow during tab-complete Currently, when the user attempts symbol completion	https://git.kern el.org/stable/c/ 107e825cc448b 7834b31e8b1b 3cf0f57426d46 d5, https://git.kern el.org/stable/c/ 33d9c814652b 971461d1e30b ead6792851c20 9e7, https://git.kern el.org/stable/c/ cfdc2fa4db5750	O-LIN-LINU-240724/3761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the Tab key, kdb will use strncpy() to insert the completed symbol into the command buffer. Unfortunately it passes the size of the source buffer rather than the destination to strncpy() with predictably horrible results. Most obviously if the command buffer is already full but cp, the cursor position, is in the middle of the buffer, then we will write past the end of the supplied buffer. Fix this by replacing the dubious strncpy() calls with memmove()/memcpy() calls plus explicit boundary checks to make sure we have enough space before we start moving characters around.	3bc6d3817240547c8ddc55fa96	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39480		
Divide By Zero	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fbdev: savage: Handle err return when savagefb_check_var failed The commit 04e5eac8f3ab("fbdev: savage: Error out if pixclock equals zero") checks the value of pixclock to avoid divide-by-zero error. However the function savagefb_probe doesn't handle the error return of savagefb_check_var. When pixclock is 0, it will cause divide-by-zero error. **CVE ID: CVE-2024-39475**	https://git.kernel.org/stable/c/32f92b0078ebf79dbe4827288e0acb50d89d3d5b, https://git.kernel.org/stable/c/4b2c67e30b4e1d2ae19dba8b8e8f3b5fd3cf8089, https://git.kernel.org/stable/c/5f446859bfa46df0ffb34149499f48a2c2d8cd95	O-LIN-LINU-240724/3762
Improper Locking	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: md/raid5: fix deadlock that raid5d() wait for	https://git.kernel.org/stable/c/098d54934814dd876963abfe751c3b1cf7fbe56a, https://git.kernel.org/stable/c/151f66bb618d1	O-LIN-LINU-240724/3763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			itself to clear MD_SB_CHANGE_PENDING Xiao reported that lvm2 test lvconvert-raid-takeover.sh can hang with small possibility, the root cause is exactly the same as commit bed9e27baf52 ("Revert "md/raid5: Wait for MD_SB_CHANGE_PENDING in raid5d"") However, Dan reported another hang after that, and junxiao investigated the problem and found out that this is caused by plugged bio can't issue from raid5d(). Current implementation in raid5d() has a weird dependence: 1) md_check_recovery	fd0eeb84acb61b4a9fa5d8bb0fa, https://git.kernel.org/stable/c/3f8d5e802d4cedd445f9a89be8c3fd2d0e99024b	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 raid5d() must hold 'reconfig_mutex' to clear MD_SB_CHANGE_PENDING; 2) raid5d() handles IO in a deadloop, until all IO are issued; 3) IO from raid5d() must wait for MD_SB_CHANGE_PENDING to be cleared; This behaviour is introduce before v2.6, and for consequence, if other context hold 'reconfig_mutex', and md_check_recovery() can't update super_block, then raid5d() will waste one cpu 100% by the deadloop, until 'reconfig_mutex' is released. Refer to the implementation from raid1 and raid10, fix this problem by		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			skipping issue IO if MD_SB_CHANGE_PENDING is still set after md_check_recovery(), daemon thread will be woken up when 'reconfig_mutex' is released. Meanwhile, the hang problem will be fixed as well. **CVE ID: CVE-2024-39476**		
Affected Version(s): From (including) 5.15 Up to (excluding) 5.15.162					
Allocation of Resources Without Limits or Throttling	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bcache: fix variable length array abuse in btree_iter btree_iter is used in two ways: either allocated on the stack with a fixed size MAX_BSETS, or from a mempool with a dynamic size based on the specific cache set. Previously, the struct had a fixed-length array of size MAX_BSETS which was indexed	https://git.kernel.org/stable/c/0c31344e22dd8d6b1394c6e4c41d639015bdc671, https://git.kernel.org/stable/c/2c3d7b03b658dc8bfa6112b194b67b92a87e081b, https://git.kernel.org/stable/c/3a861560ccb35f2a4f0a4b8207fa7c2a35fc7f31	O-LIN-LINU-240724/3764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			out-of-bounds for the dynamically-sized iterators, which causes UBSAN to complain. This patch uses the same approach as in bcachefs's sort_iter and splits the iterator into a btree_iter with a flexible array member and a btree_iter_stack which embeds a btree_iter as well as a fixed-length data array. **CVE ID: CVE-2024-39482**		
Allocation of Resources Without Limits or Throttling	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mmc: davinci: Don't strip remove function when driver is builtin Using __exit for the remove function results in the remove callback being discarded with CONFIG_MMC_DAVINCI=y. When such	https://git.kernel.org/stable/c/1d5ed0efe51d36b9ae9b64f133bf41cdbf56f584, https://git.kernel.org/stable/c/55c421b364482b61c4c45313a535e61ed5ae4ea3, https://git.kernel.org/stable/c/5ee241f72edc6dce5051a5f100eab6cc019d873e	O-LIN-LINU-240724/3765

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
			a device gets unbound (e.g. using sysfs or hotplug), the driver is just removed without the cleanup being performed. This results in resource leaks. Fix it by compiling in the remove callback unconditionally. This also fixes a W=1 modpost warning: WARNING: modpost: drivers/mmc/host/davinci_mmc: section mismatch in reference: davinci_mmcsd_driver+0x10 (section: .data) -> davinci_mmcsd_remove (section: .exit.text) **CVE ID: CVE-2024-39484**		
Affected Version(s): From (including) 5.4 Up to (excluding) 5.4.278					
Buffer Copy without Checking Size of	05-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/107e825cc448b7834b31e8b1b3cf0f57426d46	O-LIN-LINU-240724/3766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			kdb: Fix buffer overflow during tab-complete Currently, when the user attempts symbol completion with the Tab key, kdb will use strncpy() to insert the completed symbol into the command buffer. Unfortunately it passes the size of the source buffer rather than the destination to strncpy() with predictably horrible results. Most obviously if the command buffer is already full but cp, the cursor position, is in the middle of the buffer, then we will write past the end of the supplied buffer. Fix this by replacing the dubious strncpy() calls with	d5, https://git.kernel.org/stable/c/33d9c814652b971461d1e30bead6792851c209e7, https://git.kernel.org/stable/c/cfdc2fa4db57503bc6d3817240547c8ddc55fa96	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memmove()/memcpy() calls plus explicit boundary checks to make sure we have enough space before we start moving characters around. **CVE ID: CVE-2024-39480**		
Divide By Zero	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fbdev: savage: Handle err return when savagefb_check_var failed The commit 04e5eac8f3ab("fbdev: savage: Error out if pixclock equals zero") checks the value of pixclock to avoid divide-by-zero error. However the function savagefb_probe doesn't handle the error return of savagefb_check_var. When pixclock is 0, it will cause divide-by-zero error.	https://git.kernel.org/stable/c/32f92b0078ebf79dbe4827288e0acb50d89d3d5b, https://git.kernel.org/stable/c/4b2c67e30b4e1d2ae19dba8b8e8f3b5fd3cf8089, https://git.kernel.org/stable/c/5f446859bfa46df0ffb34149499f48a2c2d8cd95	O-LIN-LINU-240724/3767

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-39475		
Improper Locking	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: md/raid5: fix deadlock that raid5d() wait for itself to clear MD_SB_CHANGE_PENDING Xiao reported that lvm2 test lvconvert-raid-takeover.sh can hang with small possibility, the root cause is exactly the same as commit bed9e27baf52 ("Revert "md/raid5: Wait for MD_SB_CHANGE_PENDING in raid5d"") However, Dan reported another hang after that, and junxiao investigated the problem and found out that this is caused by	https://git.kernel.org/stable/c/098d54934814dd876963abfe751c3b1cf7fbe56a, https://git.kernel.org/stable/c/151f66bb618d1fd0eeb84acb61b4a9fa5d8bb0fa, https://git.kernel.org/stable/c/3f8d5e802d4cedd445f9a89be8c3fd2d0e99024b	O-LIN-LINU-240724/3768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			plugged bio can't issue from raid5d(). Current implementation in raid5d() has a weird dependence: 1) md_check_recovery() from raid5d() must hold 'reconfig_mutex' to clear MD_SB_CHANGE_PENDING; 2) raid5d() handles IO in a deadloop, until all IO are issued; 3) IO from raid5d() must wait for MD_SB_CHANGE_PENDING to be cleared; This behaviour is introduce before v2.6, and for consequence, if other context hold 'reconfig_mutex', and md_check_recovery() can't update super_block, then raid5d() will waste		

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			one cpu 100% by the deadloop, until 'reconfig_mutex' is released. Refer to the implementation from raid1 and raid10, fix this problem by skipping issue IO if MD_SB_CHANGE_PENDING is still set after md_check_recovery(), daemon thread will be woken up when 'reconfig_mutex' is released. Meanwhile, the hang problem will be fixed as well. **CVE ID: CVE-2024-39476**		
Affected Version(s): From (including) 6.1 Up to (excluding) 6.1.94					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: kdb: Fix buffer overflow during tab-complete Currently, when the user attempts symbol completion	https://git.kernel.org/stable/c/107e825cc448b7834b31e8b1b3cf0f57426d46d5, https://git.kernel.org/stable/c/33d9c814652b971461d1e30bead6792851c209e7, https://git.kernel.org/stable/c/cfdc2fa4db5750	O-LIN-LINU-240724/3769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the Tab key, kdb will use strncpy() to insert the completed symbol into the command buffer. Unfortunately it passes the size of the source buffer rather than the destination to strncpy() with predictably horrible results. Most obviously if the command buffer is already full but cp, the cursor position, is in the middle of the buffer, then we will write past the end of the supplied buffer. Fix this by replacing the dubious strncpy() calls with memmove()/memcpy() calls plus explicit boundary checks to make sure we have enough space before we start moving characters around.	3bc6d3817240547c8ddc55fa96	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-39480		
Divide By Zero	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fbdev: savage: Handle err return when savagefb_check_var failed The commit 04e5eac8f3ab("fbdev: savage: Error out if pixclock equals zero") checks the value of pixclock to avoid divide-by-zero error. However the function savagefb_probe doesn't handle the error return of savagefb_check_var. When pixclock is 0, it will cause divide-by-zero error. **CVE ID: CVE-2024-39475**	https://git.kernel.org/stable/c/32f92b0078ebf79dbe4827288e0acb50d89d3d5b, https://git.kernel.org/stable/c/4b2c67e30b4e1d2ae19dba8b8e8f3b5fd3cf8089, https://git.kernel.org/stable/c/5f446859bfa46df0ffb34149499f48a2c2d8cd95	O-LIN-LINU-240724/3770
Improper Locking	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: md/raid5: fix deadlock that raid5d() wait for	https://git.kernel.org/stable/c/098d54934814dd876963abfe751c3b1cf7fbe56a, https://git.kernel.org/stable/c/151f66bb618d1	O-LIN-LINU-240724/3771

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
			itself to clear MD_SB_CHANGE_PENDING Xiao reported that lvm2 test lvconvert-raid-takeover.sh can hang with small possibility, the root cause is exactly the same as commit bed9e27baf52 ("Revert "md/raid5: Wait for MD_SB_CHANGE_PENDING in raid5d"") However, Dan reported another hang after that, and junxiao investigated the problem and found out that this is caused by plugged bio can't issue from raid5d(). Current implementation in raid5d() has a weird dependence: 1) md_check_recovery	fd0eeb84acb61b4a9fa5d8bb0fa, https://git.kernel.org/stable/c/3f8d5e802d4cedd445f9a89be8c3fd2d0e99024b	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 raid5d() must hold 'reconfig_mutex' to clear MD_SB_CHANGE_PENDING; 2) raid5d() handles IO in a deadloop, until all IO are issued; 3) IO from raid5d() must wait for MD_SB_CHANGE_PENDING to be cleared; This behaviour is introduce before v2.6, and for consequence, if other context hold 'reconfig_mutex', and md_check_recovery() can't update super_block, then raid5d() will waste one cpu 100% by the deadloop, until 'reconfig_mutex' is released. Refer to the implementation from raid1 and raid10, fix this problem by		

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			skipping issue IO if MD_SB_CHANGE_PENDING is still set after md_check_recovery(), daemon thread will be woken up when 'reconfig_mutex' is released. Meanwhile, the hang problem will be fixed as well. **CVE ID: CVE-2024-39476**		
N/A	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: media: mc: Fix graph walk in media_pipeline_start The graph walk tries to follow all links, even if they are not between pads. This causes a crash with, e.g. a MEDIA_LNK_FL_ANCILLARY_LINK link. Fix this by allowing the walk to proceed only for MEDIA_LNK_FL_DATA_LINK links.	https://git.kernel.org/stable/c/788fd0f11e45ae8d3a8ebbd3452a6e83f92db376, https://git.kernel.org/stable/c/8a9d420149c477e7c97fbd6453704e4612bdd3fa, https://git.kernel.org/stable/c/bee9440bc0b6b3b7432f7bfde28656262a3484a2	O-LIN-LINU-240724/3772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39481		
Allocation of Resources Without Limits or Throttling	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bcache: fix variable length array abuse in btree_iter btree_iter is used in two ways: either allocated on the stack with a fixed size MAX_BSETS, or from a mempool with a dynamic size based on the specific cache set. Previously, the struct had a fixed-length array of size MAX_BSETS which was indexed out-of-bounds for the dynamically-sized iterators, which causes UBSAN to complain. This patch uses the same approach as in bcachefs's sort_iter and splits the iterator into a btree_iter with a	https://git.kernel.org/stable/c/0c31344e22dd8d6b1394c6e4c41d639015bdc671, https://git.kernel.org/stable/c/2c3d7b03b658dc8bfa6112b194b67b92a87e081b, https://git.kernel.org/stable/c/3a861560ccb35f2a4f0a4b8207fa7c2a35fc7f31	O-LIN-LINU-240724/3773

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			flexible array member and a btree_iter_stack which embeds a btree_iter as well as a fixed-length data array. **CVE ID: CVE-2024-39482**		
Affected Version(s): From (including) 6.1 Up to (excluding) 6.1.95					
Allocation of Resources Without Limits or Throttling	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/vmalloc: fix vmalloc which may return null if called with __GFP_NOFAIL commit a421ef303008 ("mm: allow !GFP_KERNEL allocations for kvmalloc") includes support for __GFP_NOFAIL, but it presents a conflict with commit dd544141b9eb ("vmalloc: back off when the current task is OOM-killed"). A possible scenario is as follows:	https://git.kernel.org/stable/c/198a80833e3421d4c9820a4ae907120adf598c91, https://git.kernel.org/stable/c/758678b65164b2158fc1de411092191cb3c394d4, https://git.kernel.org/stable/c/8e0545c83d672750632f46e3f9ad95c48c91a0fc	O-LIN-LINU-240724/3774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			process-a __vmalloc_node_range(GFP_KERNEL | __GFP_NOFAIL) __vmalloc_area_node() vm_area_alloc_pages() --> oom-killer send SIGKILL to process-a if (fatal_signal_pending(current)) break; --> return NULL; To fix this, do not check fatal_signal_pending() in vm_area_alloc_pages() if __GFP_NOFAIL set. This issue occurred during OPLUS KASAN TEST. Below is part of the log -> oom-killer sends signal to process [65731.222840] [T1308] oom-kill:constraint=CONSTRAINT_NONE,nodemask=(null),cp		

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uset=/,mems_allowed=0,global_oom,task_memcg=/apps/uid_10198,task=gs.intelligence,pid=32454,uid=10198 [65731.259685] [T32454] Call trace: [65731.259698] [T32454] dump_backtrace+0xf4/0x118 [65731.259734] [T32454] show_stack+0x18/0x24 [65731.259756] [T32454] dump_stack_lvl+0x60/0x7c [65731.259781] [T32454] dump_stack+0x18/0x38 [65731.259800] [T32454] mrdump_common_die+0x250/0x39c [mrdump] [65731.259936] [T32454] ipanic_die+0x20/0x34 [mrdump] [65731.260019] [T32454] atomic_notifier_call_chain+0xb4/0xfc [65731.260047] [T32454]		

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			notify_die+0x114/0x198 [65731.260073] [T32454] die+0xf4/0x5b4 [65731.260098] [T32454] die_kernel_fault+0x80/0x98 [65731.260124] [T32454] __do_kernel_fault+0x160/0x2a8 [65731.260146] [T32454] do_bad_area+0x68/0x148 [65731.260174] [T32454] do_mem_abort+0x151c/0x1b34 [65731.260204] [T32454] el1_abort+0x3c/0x5c [65731.260227] [T32454] el1h_64_sync_handler+0x54/0x90 [65731.260248] [T32454] el1h_64_sync+0x68/0x6c [65731.260269] [T32454] z_erofs_decompress_queue+0x7f0/0x2258		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			--> be->decompressed_pages = kvcalloc(be->nr_pages, sizeof(struct page *), GFP_KERNEL | __GFP_NOFAIL); kernel panic by NULL pointer dereference. erofs assume kvmalloc with __GFP_NOFAIL never return NULL. [65731.260293] [T32454] z_erofs_runqueue+0xf30/0x104c [65731.260314] [T32454] z_erofs_readahead+0x4f0/0x968 [65731.260339] [T32454] read_pages+0x170/0xadc [65731.260364] [T32454] page_cache_ra_unbounded+0x874/0xf30 [65731.260388] [T32454] page_cache_ra_order+0x24c/0x714 [65731.260411] [T32454] filemap_fault+0xbf0/0x1a74 [65731.260437] [T32454]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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_fault+0xd0/0x33c [65731.260462] [T32454] handle_mm_fault+0xf74/0x3fe0 [65731.260486] [T32454] do_mem_abort+0x54c/0x1b34 [65731.260509] [T32454] el0_da+0x44/0x94 [65731.260531] [T32454] el0t_64_sync_handler+0x98/0xb4 [65731.260553] [T32454] el0t_64_sync+0x198/0x19c **CVE ID: CVE-2024-39474**		
Allocation of Resources Without Limits or Throttling	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mmc: davinci: Don't strip remove function when driver is builtin Using __exit for the remove function results in the remove callback being discarded with CONFIG_MMC_DAV	https://git.kernel.org/stable/c/1d5ed0efe51d36b9ae9b64f133bf41cdbf56f584, https://git.kernel.org/stable/c/55c421b364482b61c4c45313a535e61ed5ae4ea3, https://git.kernel.org/stable/c/5ee241f72edc6dce5051a5f100eab6cc019d873e	O-LIN-LINU-240724/3775

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			INCI=y. When such a device gets unbound (e.g. using sysfs or hotplug), the driver is just removed without the cleanup being performed. This results in resource leaks. Fix it by compiling in the remove callback unconditionally. This also fixes a W=1 modpost warning: WARNING: modpost: drivers/mmc/host/davinci_mmc: section mismatch in reference: davinci_mmcsd_driver+0x10 (section: .data) ->davinci_mmcsd_remove (section: .exit.text) **CVE ID: CVE-2024-39484**		
Affected Version(s): From (including) 6.6 Up to (excluding) 6.6.34					
N/A	05-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/5bc9de065b8bb9b8dd8799ecb4	O-LIN-LINU-240724/3776

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
			drm/i915/hwmon: Get rid of devm When both hwmon and hwmon drvdata (on which hwmon depends) are device managed resources, the expectation, on device unbind, is that hwmon will be released before drvdata. However, in i915 there are two separate code paths, which both release either drvdata or hwmon and either can be released before the other. These code paths (for device unbind) are as follows (see also the bug referenced below): Call Trace: release_nodes+0x11/0x70 devres_release_group+0xb2/0x110 component_unbind_all+0x8d/0xa0 component_del+0xa5/0x140	592d0403b54281, https://git.kernel.org/stable/c/ce5a22d22db691d14516c3b8fdbf69139eb2ea8f, https://git.kernel.org/stable/c/cfa73607eb21a4ce1d6294a2c5733628897b48a2	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intel_pxp_tee_component_fini+0x29/0x40 [i915] intel_pxp_fini+0x33/0x80 [i915] i915_driver_remove+0x4c/0x120 [i915] i915_pci_remove+0x19/0x30 [i915] pci_device_remove+0x32/0xa0 device_release_driver_internal+0x19c/0x200 unbind_store+0x9c/0xb0 and Call Trace: release_nodes+0x11/0x70 devres_release_all+0x8a/0xc0 device_unbind_cleanup+0x9/0x70 device_release_driver_internal+0x1c1/0x200 unbind_store+0x9c/0xb0 This means that in i915, if use devm, we cannot gurantee that hwmon will		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			always be released before drvdata. Which means that we have a uaf if hwmon sysfs is accessed when drvdata has been released but hwmon hasn't. The only way out of this seems to be do get rid of devm_ and release/free everything explicitly during device unbind. v2: Change commit message and other minor code changes v3: Cleanup from i915_hwmon_register on error (Armin Wolf) v4: Eliminate potential static analyzer warning (Rodrigo) Eliminate fetch_and_zero (Jani) v5: Restore previous logic for ddat_gt->hwmon_dev error return (Andi) **CVE ID: CVE-2024-39479**		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	05-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: kdb: Fix buffer overflow during tab-complete Currently, when the user attempts symbol completion with the Tab key, kdb will use strncpy() to insert the completed symbol into the command buffer. Unfortunately it passes the size of the source buffer rather than the destination to strncpy() with predictably horrible results. Most obviously if the command buffer is already full but cp, the cursor position, is in the middle of the buffer, then we will write past the end of the supplied buffer.	https://git.kernel.org/stable/c/107e825cc448b7834b31e8b1b3cf0f57426d46d5, https://git.kernel.org/stable/c/33d9c814652b971461d1e30bead6792851c209e7, https://git.kernel.org/stable/c/cfdc2fa4db57503bc6d3817240547c8ddc55fa96	O-LIN-LINU-240724/3777

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
			Fix this by replacing the dubious strncpy() calls with memmove()/memcpy() calls plus explicit boundary checks to make sure we have enough space before we start moving characters around. **CVE ID: CVE-2024-39480**		
NULL Pointer Dereference	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: ipc4-topology: Fix input format query of process modules without base extension If a process module does not have base config extension then the same format applies to all of it's inputs and the process->base_config_ext is NULL, causing NULL dereference when specifically crafted topology and	https://git.kernel.org/stable/c/9e16f17a2a0e97b43538b272e7071537a3e03368, https://git.kernel.org/stable/c/e3ae00ee238bce6cfa5ad935c921181c14d18fd6, https://git.kernel.org/stable/c/ffa077b2f6ad124ec3d23fbddc5e4b0ff2647af8	O-LIN-LINU-240724/3778

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
			sequences used. **CVE ID: CVE-2024-39473**		
Allocation of Resources Without Limits or Throttling	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/vmalloc: fix vmalloc which may return null if called with __GFP_NOFAIL commit a421ef303008 ("mm: allow !GFP_KERNEL allocations for kvmalloc") includes support for __GFP_NOFAIL, but it presents a conflict with commit dd544141b9eb ("vmalloc: back off when the current task is OOM-killed"). A possible scenario is as follows: process-a __vmalloc_node_range(GFP_KERNEL | __GFP_NOFAIL) __vmalloc_area_node()	https://git.kernel.org/stable/c/198a80833e3421d4c9820a4ae907120adf598c91, https://git.kernel.org/stable/c/758678b65164b2158fc1de411092191cb3c394d4, https://git.kernel.org/stable/c/8e0545c83d672750632f46e3f9ad95c48c91a0fc	O-LIN-LINU-240724/3779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vm_area_alloc_pages() --> oom-killer send SIGKILL to process-a if (fatal_signal_pending(current)) break; --> return NULL; To fix this, do not check fatal_signal_pending() in vm_area_alloc_pages() if __GFP_NOFAIL set. This issue occurred during OPLUS KASAN TEST. Below is part of the log -> oom-killer sends signal to process [65731.222840] [T1308] oom-kill:constraint=CONSTRAINT_NONE,nodemask=(null),cpuset=/,mems_allowed=0,global_oom,task_memcg=/apps/uid_10198,task=gs.intelligence,pid=32454,uid=10198		

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[65731.259685] [T32454] Call trace: [65731.259698] [T32454] dump_backtrace+0xf4/0x118 [65731.259734] [T32454] show_stack+0x18/0x24 [65731.259756] [T32454] dump_stack_lvl+0x60/0x7c [65731.259781] [T32454] dump_stack+0x18/0x38 [65731.259800] [T32454] mrdump_common_die+0x250/0x39c [mrdump] [65731.259936] [T32454] ipanic_die+0x20/0x34 [mrdump] [65731.260019] [T32454] atomic_notifier_call_chain+0xb4/0xfc [65731.260047] [T32454] notify_die+0x114/0x198 [65731.260073] [T32454] die+0xf4/0x5b4 [65731.260098] [T32454]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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_kernel_fault+0x80/0x98 [65731.260124] [T32454] __do_kernel_fault+0x160/0x2a8 [65731.260146] [T32454] do_bad_area+0x68/0x148 [65731.260174] [T32454] do_mem_abort+0x151c/0x1b34 [65731.260204] [T32454] el1_abort+0x3c/0x5c [65731.260227] [T32454] el1h_64_sync_handler+0x54/0x90 [65731.260248] [T32454] el1h_64_sync+0x68/0x6c [65731.260269] [T32454] z_erofs_decompress_queue+0x7f0/0x2258 --> be->decompressed_pages = kvcalloc(be->nr_pages, sizeof(struct page *), GFP_KERNEL | __GFP_NOFAIL);		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel panic by NULL pointer dereference. erofs assume kvmalloc with __GFP_NOFAIL never return NULL. [65731.260293] [T32454] z_erofs_runqueue+0xf30/0x104c [65731.260314] [T32454] z_erofs_readahead+0x4f0/0x968 [65731.260339] [T32454] read_pages+0x170/0xadc [65731.260364] [T32454] page_cache_ra_unbounded+0x874/0xf30 [65731.260388] [T32454] page_cache_ra_order+0x24c/0x714 [65731.260411] [T32454] filemap_fault+0xbf0/0x1a74 [65731.260437] [T32454] __do_fault+0xd0/0x33c [65731.260462] [T32454] handle_mm_fault+0xf74/0x3fe0		

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[65731.260486] [T32454] do_mem_abort+0x54c/0x1b34 [65731.260509] [T32454] el0_da+0x44/0x94 [65731.260531] [T32454] el0t_64_sync_handler+0x98/0xb4 [65731.260553] [T32454] el0t_64_sync+0x198/0x19c **CVE ID: CVE-2024-39474**		
Divide By Zero	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fbdev: savage: Handle err return when savagefb_check_var failed The commit 04e5eac8f3ab("fbdev: savage: Error out if pixclock equals zero") checks the value of pixclock to avoid divide-by-zero error. However the function savagefb_probe	https://git.kernel.org/stable/c/32f92b0078ebf79dbe4827288e0acb50d89d3d5b, https://git.kernel.org/stable/c/4b2c67e30b4e1d2ae19dba8b8e8f3b5fd3cf8089, https://git.kernel.org/stable/c/5f446859bfa46df0ffb34149499f48a2c2d8cd95	O-LIN-LINU-240724/3780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			doesn't handle the error return of savagefb_check_var . When pixclock is 0, it will cause divide-by-zero error. **CVE ID: CVE-2024-39475**		
Improper Locking	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: md/raid5: fix deadlock that raid5d() wait for itself to clear MD_SB_CHANGE_PENDING Xiao reported that lvm2 test lvconvert-raid-takeover.sh can hang with small possibility, the root cause is exactly the same as commit bed9e27baf52 ("Revert "md/raid5: Wait for MD_SB_CHANGE_PENDING in raid5d"") However, Dan reported another hang after that, and	https://git.kernel.org/stable/c/098d54934814dd876963abfe751c3b1cf7fbe56a, https://git.kernel.org/stable/c/151f66bb618d1fd0eeb84acb61b4a9fa5d8bb0fa, https://git.kernel.org/stable/c/3f8d5e802d4cedd445f9a89be8c3fd2d0e99024b	O-LIN-LINU-240724/3781

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
			junxiao investigated the problem and found out that this is caused by plugged bio can't issue from raid5d(). Current implementation in raid5d() has a weird dependence: 1) md_check_recovery() from raid5d() must hold 'reconfig_mutex' to clear MD_SB_CHANGE_PENDING; 2) raid5d() handles IO in a deadloop, until all IO are issued; 3) IO from raid5d() must wait for MD_SB_CHANGE_PENDING to be cleared; This behaviour is introduce before v2.6, and for consequence, if other context hold 'reconfig_mutex',		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 md_check_recovery () can't update super_block, then raid5d() will waste one cpu 100% by the deadloop, until 'reconfig_mutex' is released. Refer to the implementation from raid1 and raid10, fix this problem by skipping issue IO if MD_SB_CHANGE_PENDING is still set after md_check_recovery (), daemon thread will be woken up when 'reconfig_mutex' is released. Meanwhile, the hang problem will be fixed as well. **CVE ID: CVE-2024-39476**		
N/A	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: media: mc: Fix graph walk in media_pipeline_start	https://git.kernel.org/stable/c/788fd0f11e45ae8d3a8ebbd3452a6e83f92db376, https://git.kernel.org/stable/c/8a9d420149c477e7c97fbd6453704e4612bdd	O-LIN-LINU-240724/3782

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 graph walk tries to follow all links, even if they are not between pads. This causes a crash with, e.g. a MEDIA_LNK_FL_ANCILLARY_LINK link. Fix this by allowing the walk to proceed only for MEDIA_LNK_FL_DATA_LINK links. **CVE ID: CVE-2024-39481**	3fa, https://git.kernel.org/stable/c/bee9440bc0b6b3b7432f7bfde28656262a3484a2	
Allocation of Resources Without Limits or Throttling	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bcache: fix variable length array abuse in btree_iter btree_iter is used in two ways: either allocated on the stack with a fixed size MAX_BSETS, or from a mempool with a dynamic size based on the specific cache set. Previously, the struct had a fixed-length array of	https://git.kernel.org/stable/c/0c31344e22dd8d6b1394c6e4c41d639015bdc671, https://git.kernel.org/stable/c/2c3d7b03b658dc8bfa6112b194b67b92a87e081b, https://git.kernel.org/stable/c/3a861560ccb35f2a4f0a4b8207fa7c2a35fc7f31	O-LIN-LINU-240724/3783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			size MAX_BSETS which was indexed out-of-bounds for the dynamically-sized iterators, which causes UBSAN to complain. This patch uses the same approach as in bcachefs's sort_iter and splits the iterator into a btree_iter with a flexible array member and a btree_iter_stack which embeds a btree_iter as well as a fixed-length data array. **CVE ID: CVE-2024-39482**		
N/A	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: KVM: SVM: WARN on vNMI + NMI window iff NMIs are outright masked When requesting an NMI window, WARN on vNMI support being enabled if and	https://git.kernel.org/stable/c/1d87cf2eba46deaff6142366127f2323de9f84d1, https://git.kernel.org/stable/c/b4bd556467477420ee3a91fbcba73c579669edc6, https://git.kernel.org/stable/c/f79edaf7370986d73d204b36c	O-LIN-LINU-240724/3784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			only if NMIs are actually masked, i.e. if the vCPU is already handling an NMI. KVM's ABI for NMIs that arrive simultanesouly (from KVM's point of view) is to inject one NMI and pend the other. When using vNMI, KVM pends the second NMI simply by setting V_NMI_PENDING, and lets the CPU do the rest (hardware automatically sets V_NMI_BLOCKING when an NMI is injected). However, if KVM can't immediately inject an NMI, e.g. because the vCPU is in an STI shadow or is running with GIF=0, then KVM will request an NMI window and trigger the WARN (but still function correctly). Whether or not the GIF=0 case makes	50cc563a4c0f356	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sense is debatable, as the intent of KVM's behavior is to provide functionality that is as close to real hardware as possible. E.g. if two NMIs are sent in quick succession, the probability of both NMIs arriving in an STI shadow is infinitesimally low on real hardware, but significantly larger in a virtual environment, e.g. if the vCPU is preempted in the STI shadow. For GIF=0, the argument isn't as clear cut, because the window where two NMIs can collide is much larger in bare metal (though still small). That said, KVM should not have divergent behavior for the GIF=0 case based on whether or not vNMI support is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabled. And KVM has allowed simultaneous NMIs with GIF=0 for over a decade, since commit 7460fb4a3400 ("KVM: Fix simultaneous NMIs"). I.e. KVM's GIF=0 handling shouldn't be modified without a *really* good reason to do so, and if KVM's behavior were to be modified, it should be done irrespective of vNMI support. **CVE ID: CVE-2024-39483**		
Allocation of Resources Without Limits or Throttling	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mmc: davinci: Don't strip remove function when driver is builtin Using __exit for the remove function results in the remove callback being discarded with CONFIG_MMC_DAV	https://git.kernel.org/stable/c/1d5ed0efe51d36b9ae9b64f133bf41cdbf56f584, https://git.kernel.org/stable/c/55c421b364482b61c4c45313a535e61ed5ae4ea3, https://git.kernel.org/stable/c/5ee241f72edc6dce5051a5f100eab6cc019d873e	O-LIN-LINU-240724/3785

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
			INCI=y. When such a device gets unbound (e.g. using sysfs or hotplug), the driver is just removed without the cleanup being performed. This results in resource leaks. Fix it by compiling in the remove callback unconditionally. This also fixes a W=1 modpost warning: WARNING: modpost: drivers/mmc/host/davinci_mmc: section mismatch in reference: davinci_mmcsd_driver+0x10 (section: .data) -> davinci_mmcsd_remove (section: .exit.text) **CVE ID: CVE-2024-39484**		
Affected Version(s): From (including) 6.9 Up to (excluding) 6.9.5					
N/A	05-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/5bc9de065b8bb9b8dd8799ecb4	O-LIN-LINU-240724/3786

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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/i915/hwmon: Get rid of devm When both hwmon and hwmon drvdata (on which hwmon depends) are device managed resources, the expectation, on device unbind, is that hwmon will be released before drvdata. However, in i915 there are two separate code paths, which both release either drvdata or hwmon and either can be released before the other. These code paths (for device unbind) are as follows (see also the bug referenced below): Call Trace: release_nodes+0x11/0x70 devres_release_group+0xb2/0x110 component_unbind_all+0x8d/0xa0 component_del+0xa5/0x140	592d0403b54281, https://git.kernel.org/stable/c/ce5a22d22db691d14516c3b8fdbf69139eb2ea8f, https://git.kernel.org/stable/c/cfa73607eb21a4ce1d6294a2c5733628897b48a2	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intel_pxp_tee_component_fini+0x29/0x40 [i915] intel_pxp_fini+0x33/0x80 [i915] i915_driver_remove+0x4c/0x120 [i915] i915_pci_remove+0x19/0x30 [i915] pci_device_remove+0x32/0xa0 device_release_driver_internal+0x19c/0x200 unbind_store+0x9c/0xb0 and Call Trace: release_nodes+0x11/0x70 devres_release_all+0x8a/0xc0 device_unbind_cleanup+0x9/0x70 device_release_driver_internal+0x1c1/0x200 unbind_store+0x9c/0xb0 This means that in i915, if use devm, we cannot gurantee that hwmon will		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			always be released before drvdata. Which means that we have a uaf if hwmon sysfs is accessed when drvdata has been released but hwmon hasn't. The only way out of this seems to be do get rid of devm_ and release/free everything explicitly during device unbind. v2: Change commit message and other minor code changes v3: Cleanup from i915_hwmon_register on error (Armin Wolf) v4: Eliminate potential static analyzer warning (Rodrigo) Eliminate fetch_and_zero (Jani) v5: Restore previous logic for ddat_gt->hwmon_dev error return (Andi) **CVE ID: CVE-2024-39479**		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	05-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: kdb: Fix buffer overflow during tab-complete Currently, when the user attempts symbol completion with the Tab key, kdb will use strncpy() to insert the completed symbol into the command buffer. Unfortunately it passes the size of the source buffer rather than the destination to strncpy() with predictably horrible results. Most obviously if the command buffer is already full but cp, the cursor position, is in the middle of the buffer, then we will write past the end of the supplied buffer.	https://git.kernel.org/stable/c/107e825cc448b7834b31e8b1b3cf0f57426d46d5, https://git.kernel.org/stable/c/33d9c814652b971461d1e30bead6792851c209e7, https://git.kernel.org/stable/c/cfdc2fa4db57503bc6d3817240547c8ddc55fa96	O-LIN-LINU-240724/3787

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
			Fix this by replacing the dubious strncpy() calls with memmove()/memcpy() calls plus explicit boundary checks to make sure we have enough space before we start moving characters around. **CVE ID: CVE-2024-39480**		
NULL Pointer Dereference	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: ipc4-topology: Fix input format query of process modules without base extension If a process module does not have base config extension then the same format applies to all of it's inputs and the process->base_config_ext is NULL, causing NULL dereference when specifically crafted topology and	https://git.kernel.org/stable/c/9e16f17a2a0e97b43538b272e7071537a3e03368, https://git.kernel.org/stable/c/e3ae00ee238bce6cfa5ad935c921181c14d18fd6, https://git.kernel.org/stable/c/ffa077b2f6ad124ec3d23fbddc5e4b0ff2647af8	O-LIN-LINU-240724/3788

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
			sequences used. **CVE ID: CVE-2024-39473**		
Allocation of Resources Without Limits or Throttling	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/vmalloc: fix vmalloc which may return null if called with __GFP_NOFAIL commit a421ef303008 ("mm: allow !GFP_KERNEL allocations for kvmalloc") includes support for __GFP_NOFAIL, but it presents a conflict with commit dd544141b9eb ("vmalloc: back off when the current task is OOM-killed"). A possible scenario is as follows: process-a __vmalloc_node_range(GFP_KERNEL | __GFP_NOFAIL) __vmalloc_area_node()	https://git.kernel.org/stable/c/198a80833e3421d4c9820a4ae907120adf598c91, https://git.kernel.org/stable/c/758678b65164b2158fc1de411092191cb3c394d4, https://git.kernel.org/stable/c/8e0545c83d672750632f46e3f9ad95c48c91a0fc	O-LIN-LINU-240724/3789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vm_area_alloc_pages() --> oom-killer send SIGKILL to process-a if (fatal_signal_pending(current)) break; --> return NULL; To fix this, do not check fatal_signal_pending() in vm_area_alloc_pages() if __GFP_NOFAIL set. This issue occurred during OPLUS KASAN TEST. Below is part of the log -> oom-killer sends signal to process [65731.222840] [T1308] oom-kill:constraint=CONSTRAINT_NONE,nodemask=(null),cpuset=/,mems_allowed=0,global_oom,task_memcg=/apps/uid_10198,task=gs.intelligence,pid=32454,uid=10198		

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[65731.259685] [T32454] Call trace: [65731.259698] [T32454] dump_backtrace+0xf4/0x118 [65731.259734] [T32454] show_stack+0x18/0x24 [65731.259756] [T32454] dump_stack_lvl+0x60/0x7c [65731.259781] [T32454] dump_stack+0x18/0x38 [65731.259800] [T32454] mrdump_common_die+0x250/0x39c [mrdump] [65731.259936] [T32454] ipanic_die+0x20/0x34 [mrdump] [65731.260019] [T32454] atomic_notifier_call_chain+0xb4/0xfc [65731.260047] [T32454] notify_die+0x114/0x198 [65731.260073] [T32454] die+0xf4/0x5b4 [65731.260098] [T32454]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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_kernel_fault+0x80/0x98 [65731.260124] [T32454] __do_kernel_fault+0x160/0x2a8 [65731.260146] [T32454] do_bad_area+0x68/0x148 [65731.260174] [T32454] do_mem_abort+0x151c/0x1b34 [65731.260204] [T32454] el1_abort+0x3c/0x5c [65731.260227] [T32454] el1h_64_sync_handler+0x54/0x90 [65731.260248] [T32454] el1h_64_sync+0x68/0x6c [65731.260269] [T32454] z_erofs_decompress_queue+0x7f0/0x2258 --> be->decompressed_pages = kvcalloc(be->nr_pages, sizeof(struct page *), GFP_KERNEL | __GFP_NOFAIL);		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel panic by NULL pointer dereference. erofs assume kvmalloc with __GFP_NOFAIL never return NULL. [65731.260293] [T32454] z_erofs_runqueue+0xf30/0x104c [65731.260314] [T32454] z_erofs_readahead+0x4f0/0x968 [65731.260339] [T32454] read_pages+0x170/0xadc [65731.260364] [T32454] page_cache_ra_unbounded+0x874/0xf30 [65731.260388] [T32454] page_cache_ra_order+0x24c/0x714 [65731.260411] [T32454] filemap_fault+0xbf0/0x1a74 [65731.260437] [T32454] __do_fault+0xd0/0x33c [65731.260462] [T32454] handle_mm_fault+0xf74/0x3fe0		

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[65731.260486] [T32454] do_mem_abort+0x54c/0x1b34 [65731.260509] [T32454] el0_da+0x44/0x94 [65731.260531] [T32454] el0t_64_sync_handler+0x98/0xb4 [65731.260553] [T32454] el0t_64_sync+0x198/0x19c **CVE ID: CVE-2024-39474**		
Divide By Zero	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fbdev: savage: Handle err return when savagefb_check_var failed The commit 04e5eac8f3ab("fbdev: savage: Error out if pixclock equals zero") checks the value of pixclock to avoid divide-by-zero error. However the function savagefb_probe	https://git.kernel.org/stable/c/32f92b0078ebf79dbe4827288e0acb50d89d3d5b, https://git.kernel.org/stable/c/4b2c67e30b4e1d2ae19dba8b8e8f3b5fd3cf8089, https://git.kernel.org/stable/c/5f446859bfa46df0ffb34149499f48a2c2d8cd95	O-LIN-LINU-240724/3790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			doesn't handle the error return of savagefb_check_var . When pixclock is 0, it will cause divide-by-zero error. **CVE ID: CVE-2024-39475**		
Improper Locking	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: md/raid5: fix deadlock that raid5d() wait for itself to clear MD_SB_CHANGE_PENDING Xiao reported that lvm2 test lvconvert-raid-takeover.sh can hang with small possibility, the root cause is exactly the same as commit bed9e27baf52 ("Revert "md/raid5: Wait for MD_SB_CHANGE_PENDING in raid5d"") However, Dan reported another hang after that, and	https://git.kernel.org/stable/c/098d54934814dd876963abfe751c3b1cf7fbe56a, https://git.kernel.org/stable/c/151f66bb618d1fd0eeb84acb61b4a9fa5d8bb0fa, https://git.kernel.org/stable/c/3f8d5e802d4cedd445f9a89be8c3fd2d0e99024b	O-LIN-LINU-240724/3791

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			junxiao investigated the problem and found out that this is caused by plugged bio can't issue from raid5d(). Current implementation in raid5d() has a weird dependence: 1) md_check_recovery() from raid5d() must hold 'reconfig_mutex' to clear MD_SB_CHANGE_PENDING; 2) raid5d() handles IO in a deadloop, until all IO are issued; 3) IO from raid5d() must wait for MD_SB_CHANGE_PENDING to be cleared; This behaviour is introduce before v2.6, and for consequence, if other context hold 'reconfig_mutex',		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 md_check_recovery () can't update super_block, then raid5d() will waste one cpu 100% by the deadloop, until 'reconfig_mutex' is released. Refer to the implementation from raid1 and raid10, fix this problem by skipping issue IO if MD_SB_CHANGE_PENDING is still set after md_check_recovery (), daemon thread will be woken up when 'reconfig_mutex' is released. Meanwhile, the hang problem will be fixed as well. **CVE ID: CVE-2024-39476**		
Allocation of Resources Without Limits or Throttling	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/hugetlb: do not call vma_add_reservation upon ENOMEM	https://git.kernel.org/stable/c/8daf9c702ee7f825f0de8600abff764acfedea13, https://git.kernel.org/stable/c/aa998f9dcb34c28448f86e8f5490f20d5eb0eac7	O-LIN-LINU-240724/3792

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
			sysbot reported a splat [1] on __unmap_hugepage_range(). This is because vma_needs_reservation() can return -ENOMEM if allocate_file_region_entries() fails to allocate the file_region struct for the reservation. Check for that and do not call vma_add_reservation() if that is the case, otherwise region_abort() and region_del() will see that we do not have any file_regions. If we detect that vma_needs_reservation() returned -ENOMEM, we clear the hugetlb_restore_reserve flag as if this reservation was still consumed, so free_huge_folio() will not increment the resv count.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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] https://lore.kernel.org/linux-mm/00000000000004096100617c58d54@google.com/T/#ma5983bc1ab18a54910da83416b3f89f3c7ee43aa **CVE ID: CVE-2024-39477**		
Allocation of Resources Without Limits or Throttling	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: crypto: starfive - Do not free stack buffer RSA text data uses variable length buffer allocated in software stack. Calling kfree on it causes undefined behaviour in subsequent operations. **CVE ID: CVE-2024-39478**	https://git.kernel.org/stable/c/5944de192663f272033501dcd322b008fca72006, https://git.kernel.org/stable/c/d7f01649f4eaf1878472d3d3f480ae1e50d98f6c	O-LIN-LINU-240724/3793
N/A	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: media: mc: Fix graph walk in media_pipeline_start	https://git.kernel.org/stable/c/788fd0f11e45ae8d3a8ebbd3452a6e83f92db376, https://git.kernel.org/stable/c/8a9d420149c477e7c97fbd645	O-LIN-LINU-240724/3794

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 graph walk tries to follow all links, even if they are not between pads. This causes a crash with, e.g. a MEDIA_LNK_FL_ANCILLARY_LINK link. Fix this by allowing the walk to proceed only for MEDIA_LNK_FL_DATA_LINK links. **CVE ID: CVE-2024-39481**	3704e4612bdd3fa, https://git.kernel.org/stable/c/bee9440bc0b6b3b7432f7bfde28656262a3484a2	
Allocation of Resources Without Limits or Throttling	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bcache: fix variable length array abuse in btree_iter btree_iter is used in two ways: either allocated on the stack with a fixed size MAX_BSETS, or from a mempool with a dynamic size based on the specific cache set. Previously, the	https://git.kernel.org/stable/c/0c31344e22dd8d6b1394c6e4c41d639015bdc671, https://git.kernel.org/stable/c/2c3d7b03b658dc8bfa6112b194b67b92a87e081b, https://git.kernel.org/stable/c/3a861560ccb35f2a4f0a4b8207fa7c2a35fc7f31	O-LIN-LINU-240724/3795

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
			struct had a fixed-length array of size MAX_BSETS which was indexed out-of-bounds for the dynamically-sized iterators, which causes UBSAN to complain. This patch uses the same approach as in bcachefs's sort_iter and splits the iterator into a btree_iter with a flexible array member and a btree_iter_stack which embeds a btree_iter as well as a fixed-length data array. **CVE ID: CVE-2024-39482**		
N/A	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: KVM: SVM: WARN on vNMI + NMI window iff NMIs are outright masked When requesting an NMI window, WARN on vNMI	https://git.kernel.org/stable/c/1d87cf2eba46deaff6142366127f2323de9f84d1, https://git.kernel.org/stable/c/b4bd556467477420ee3a91fbcba73c579669edc6, https://git.kernel.org/stable/c/f79edaf737098	O-LIN-LINU-240724/3796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			support being enabled if and only if NMIs are actually masked, i.e. if the vCPU is already handling an NMI. KVM's ABI for NMIs that arrive simultanesouly (from KVM's point of view) is to inject one NMI and pend the other. When using vNMI, KVM pends the second NMI simply by setting V_NMI_PENDING, and lets the CPU do the rest (hardware automatically sets V_NMI_BLOCKING when an NMI is injected). However, if KVM can't immediately inject an NMI, e.g. because the vCPU is in an STI shadow or is running with GIF=0, then KVM will request an NMI window and trigger the WARN (but still function correctly).	6d73d204b36c50cc563a4c0f356	

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Whether or not the GIF=0 case makes sense is debatable, as the intent of KVM's behavior is to provide functionality that is as close to real hardware as possible. E.g. if two NMIs are sent in quick succession, the probability of both NMIs arriving in an STI shadow is infinitesimally low on real hardware, but significantly larger in a virtual environment, e.g. if the vCPU is preempted in the STI shadow. For GIF=0, the argument isn't as clear cut, because the window where two NMIs can collide is much larger in bare metal (though still small). That said, KVM should not have divergent behavior for the GIF=0 case based on whether or not vNMI support 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
			enabled. And KVM has allowed simultaneous NMIs with GIF=0 for over a decade, since commit 7460fb4a3400 ("KVM: Fix simultaneous NMIs"). I.e. KVM's GIF=0 handling shouldn't be modified without a *really* good reason to do so, and if KVM's behavior were to be modified, it should be done irrespective of vNMI support. **CVE ID: CVE-2024-39483**		
Allocation of Resources Without Limits or Throttling	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mmc: davinci: Don't strip remove function when driver is builtin Using __exit for the remove function results in the remove callback being discarded with CONFIG_MMC_DAV	https://git.kernel.org/stable/c/1d5ed0efe51d36b9ae9b64f133bf41cdbf56f584, https://git.kernel.org/stable/c/55c421b364482b61c4c45313a535e61ed5ae4ea3, https://git.kernel.org/stable/c/5ee241f72edc6dce5051a5f100eab6cc019d873e	O-LIN-LINU-240724/3797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			INCI=y. When such a device gets unbound (e.g. using sysfs or hotplug), the driver is just removed without the cleanup being performed. This results in resource leaks. Fix it by compiling in the remove callback unconditionally. This also fixes a W=1 modpost warning: WARNING: modpost: drivers/mmc/host/davinci_mmc: section mismatch in reference: davinci_mmcsd_driver+0x10 (section: .data) ->davinci_mmcsd_remove (section: .exit.text) **CVE ID: CVE-2024-39484**		
Improper Initialization	05-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/1aa6cd4adfc0380fa1ccc2f146848940ff882a66,	O-LIN-LINU-240724/3798

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
			media: v4l: async: Properly re-initialise notifier entry in unregister The notifier_entry of a notifier is not re-initialised after unregistering the notifier. This leads to dangling pointers being left there so use list_del_init() to return the notifier_entry an empty list. **CVE ID: CVE-2024-39485**	https://git.kernel.org/stable/c/87100b09246202a91fce4a1562955c32229173bb, https://git.kernel.org/stable/c/9537a8425a7a0222999d5839a0b394b1e8834b4a	
Vendor: Microsoft					
Product: azure_devops_server					
Affected Version(s): 2022.1.0					
N/A	09-Jul-2024	7.6	Azure DevOps Server Spoofing Vulnerability **CVE ID: CVE-2024-35266**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35266	O-MIC-AZUR-240724/3799
N/A	09-Jul-2024	7.6	Azure DevOps Server Spoofing Vulnerability **CVE ID: CVE-2024-35267**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35267	O-MIC-AZUR-240724/3800
Product: windows					
Affected Version(s): -					
N/A	09-Jul-2024	7	In Docker Desktop before v4.29.0, an attacker who has	N/A	O-MIC-WIND-240724/3801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gained access to the Docker Desktop VM through a container breakout can further escape to the host by passing extensions and dashboard related IPC messages. Docker Desktop v4.29.0 https://docs.docker.com/desktop/release-notes/#4290 fixes the issue on MacOS, Linux and Windows with Hyper-V backend. As exploitation requires "Allow only extensions distributed through the Docker Marketplace" to be disabled, Docker Desktop v4.31.0 https://docs.docker.com/desktop/release-notes/#4310 additionally changes the default configuration to enable this setting by default. **CVE ID: CVE-2024-6222**		
Product: windows_10_1507					
Affected Version(s): * Up to (excluding) 10.0.10240.20710					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	8.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-28899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28899	O-MIC-WIND-240724/3802
Use After Free	09-Jul-2024	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability **CVE ID: CVE-2024-38053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38053	O-MIC-WIND-240724/3803
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jul-2024	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38104**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38104	O-MIC-WIND-240724/3804
Out-of-bounds Write	09-Jul-2024	8.8	Windows Imaging Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38060**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38060	O-MIC-WIND-240724/3805
N/A	09-Jul-2024	8.4	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37984	O-MIC-WIND-240724/3806
Externally Controlled Reference to a Resource in Another Sphere	09-Jul-2024	8.1	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38049	O-MIC-WIND-240724/3807

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
			CVE ID: CVE-2024-38049		
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38010**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38010	O-MIC-WIND-240724/3808
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38011**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38011	O-MIC-WIND-240724/3809
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37969**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37969	O-MIC-WIND-240724/3810
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37970**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37970	O-MIC-WIND-240724/3811
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37971**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37971	O-MIC-WIND-240724/3812
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37972**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37972	O-MIC-WIND-240724/3813

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
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37974**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37974	O-MIC-WIND-240724/3814
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37975**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37975	O-MIC-WIND-240724/3815
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37986**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37986	O-MIC-WIND-240724/3816
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37987**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37987	O-MIC-WIND-240724/3817
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37988**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37988	O-MIC-WIND-240724/3818
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37989**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37989	O-MIC-WIND-240724/3819
N/A	09-Jul-2024	7.8	Windows Filtering Platform Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/3820

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38034	lity/CVE-2024-38034	
N/A	09-Jul-2024	7.8	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability **CVE ID: CVE-2024-30079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30079	O-MIC-WIND-240724/3821
Integer Underflow (Wrap or Wraparound)	09-Jul-2024	7.8	Windows Workstation Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38050**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38050	O-MIC-WIND-240724/3822
Out-of-bounds Write	09-Jul-2024	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38051**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38051	O-MIC-WIND-240724/3823
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38052	O-MIC-WIND-240724/3824
N/A	09-Jul-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37973**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37973	O-MIC-WIND-240724/3825
Out-of-bounds Write	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/3826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38054**	guide/vulnerability/CVE-2024-38054	
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38057	O-MIC-WIND-240724/3827
Use After Free	09-Jul-2024	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38066**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38066	O-MIC-WIND-240724/3828
N/A	09-Jul-2024	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38079	O-MIC-WIND-240724/3829
N/A	09-Jul-2024	7.8	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38070**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38070	O-MIC-WIND-240724/3830
N/A	09-Jul-2024	7.5	Windows Cryptographic Services Security Feature Bypass Vulnerability **CVE ID: CVE-2024-30098**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30098	O-MIC-WIND-240724/3831

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
N/A	09-Jul-2024	7.5	DCOM Remote Cross-Session Activation Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38061	O-MIC-WIND-240724/3832
N/A	09-Jul-2024	7.5	Windows TCP/IP Information Disclosure Vulnerability **CVE ID: CVE-2024-38064**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38064	O-MIC-WIND-240724/3833
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38068**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38068	O-MIC-WIND-240724/3834
N/A	09-Jul-2024	7.5	Microsoft WS-Discovery Denial of Service Vulnerability **CVE ID: CVE-2024-38091**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38091	O-MIC-WIND-240724/3835
User Interface (UI) Misrepresentation of Critical Information	09-Jul-2024	7.5	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-38112**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112	O-MIC-WIND-240724/3836
N/A	09-Jul-2024	7.3	PowerShell Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/3837

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
			CVE ID: CVE-2024-38033	lity/CVE-2024-38033	
Integer Overflow or Wraparound	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38019**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38019	O-MIC-WIND-240724/3838
Out-of-bounds Write	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38025**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38025	O-MIC-WIND-240724/3839
Out-of-bounds Read	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38028**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38028	O-MIC-WIND-240724/3840
N/A	09-Jul-2024	7.1	Windows NTLM Spoofing Vulnerability **CVE ID: CVE-2024-30081**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30081	O-MIC-WIND-240724/3841
Improper Link Resolution Before File Access ('Link Following')	09-Jul-2024	7	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38022**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38022	O-MIC-WIND-240724/3842

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
Improper Verification of Cryptographic Signature	09-Jul-2024	7	Windows Enroll Engine Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38069**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38069	O-MIC-WIND-240724/3843
N/A	09-Jul-2024	6.8	BitLocker Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38058**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38058	O-MIC-WIND-240724/3844
Out-of-bounds Write	09-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38065**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38065	O-MIC-WIND-240724/3845
N/A	09-Jul-2024	6.7	Microsoft Windows Server Backup Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38013	O-MIC-WIND-240724/3846
Out-of-bounds Read	09-Jul-2024	6.5	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability **CVE ID: CVE-2024-38048**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38048	O-MIC-WIND-240724/3847
N/A	09-Jul-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID: CVE-2024-38030**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38030	O-MIC-WIND-240724/3848

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38101**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38101	O-MIC-WIND-240724/3849
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38102**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38102	O-MIC-WIND-240724/3850
N/A	09-Jul-2024	6.5	Windows Line Printer Daemon Service Denial of Service Vulnerability **CVE ID: CVE-2024-38027**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38027	O-MIC-WIND-240724/3851
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38105**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38105	O-MIC-WIND-240724/3852
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38055	O-MIC-WIND-240724/3853
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/3854

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
			CVE ID: CVE-2024-38056	lity/CVE-2024-38056	
N/A	09-Jul-2024	5.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID: CVE-2024-38017**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38017	O-MIC-WIND-240724/3855
N/A	09-Jul-2024	5.3	Windows iSCSI Service Denial of Service Vulnerability **CVE ID: CVE-2024-35270**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35270	O-MIC-WIND-240724/3856
N/A	09-Jul-2024	4.7	Windows Remote Access Connection Manager Information Disclosure Vulnerability **CVE ID: CVE-2024-30071**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30071	O-MIC-WIND-240724/3857
Product: windows_10_1607					
Affected Version(s): * Up to (excluding) 10.0.14393.7159					
N/A	09-Jul-2024	8.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-28899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28899	O-MIC-WIND-240724/3858
N/A	09-Jul-2024	8.8	Windows MultiPoint Services Remote Code Execution Vulnerability **CVE ID: CVE-2024-30013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30013	O-MIC-WIND-240724/3859

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jul-2024	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38104**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38104	O-MIC-WIND-240724/3860
Out-of-bounds Write	09-Jul-2024	8.8	Windows Imaging Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38060**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38060	O-MIC-WIND-240724/3861
Use After Free	09-Jul-2024	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability **CVE ID: CVE-2024-38053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38053	O-MIC-WIND-240724/3862
N/A	09-Jul-2024	8.4	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37984	O-MIC-WIND-240724/3863
Externally Controlled Reference to a Resource in Another Sphere	09-Jul-2024	8.1	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability **CVE ID: CVE-2024-38049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38049	O-MIC-WIND-240724/3864
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/3865

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38010	lity/CVE-2024-38010	
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38011**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38011	O-MIC-WIND-240724/3866
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37970**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37970	O-MIC-WIND-240724/3867
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37971**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37971	O-MIC-WIND-240724/3868
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37972**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37972	O-MIC-WIND-240724/3869
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37974**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37974	O-MIC-WIND-240724/3870
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37975**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37975	O-MIC-WIND-240724/3871

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37969**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37969	O-MIC-WIND-240724/3872
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37986**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37986	O-MIC-WIND-240724/3873
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37987**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37987	O-MIC-WIND-240724/3874
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37988**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37988	O-MIC-WIND-240724/3875
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37989**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37989	O-MIC-WIND-240724/3876
Integer Underflow (Wrap or Wraparound)	09-Jul-2024	7.8	Windows Workstation Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38050**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38050	O-MIC-WIND-240724/3877
N/A	09-Jul-2024	7.8	Windows Remote Access Connection Manager Elevation	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/3878

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
			of Privilege Vulnerability **CVE ID: CVE-2024-30079**	guide/vulnerability/CVE-2024-30079	
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38052	O-MIC-WIND-240724/3879
Out-of-bounds Write	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38054	O-MIC-WIND-240724/3880
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38057	O-MIC-WIND-240724/3881
N/A	09-Jul-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37973**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37973	O-MIC-WIND-240724/3882
N/A	09-Jul-2024	7.8	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38070	O-MIC-WIND-240724/3883

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38070		
N/A	09-Jul-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38062	O-MIC-WIND-240724/3884
N/A	09-Jul-2024	7.8	Windows Filtering Platform Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38034	O-MIC-WIND-240724/3885
Use After Free	09-Jul-2024	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38066**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38066	O-MIC-WIND-240724/3886
N/A	09-Jul-2024	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38079	O-MIC-WIND-240724/3887
Out-of-bounds Write	09-Jul-2024	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38051**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38051	O-MIC-WIND-240724/3888
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/3889

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38043	lity/CVE-2024-38043	
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38047**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38047	O-MIC-WIND-240724/3890
N/A	09-Jul-2024	7.5	Windows Cryptographic Services Security Feature Bypass Vulnerability **CVE ID: CVE-2024-30098**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30098	O-MIC-WIND-240724/3891
N/A	09-Jul-2024	7.5	Windows TCP/IP Information Disclosure Vulnerability **CVE ID: CVE-2024-38064**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38064	O-MIC-WIND-240724/3892
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38068**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38068	O-MIC-WIND-240724/3893
N/A	09-Jul-2024	7.5	DCOM Remote Cross-Session Activation Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38061	O-MIC-WIND-240724/3894
N/A	09-Jul-2024	7.5	Microsoft WS-Discovery Denial of	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/3895

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
			Service Vulnerability **CVE ID: CVE-2024-38091**	guide/vulnerability/CVE-2024-38091	
User Interface (UI) Misrepresentation of Critical Information	09-Jul-2024	7.5	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-38112**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112	O-MIC-WIND-240724/3896
N/A	09-Jul-2024	7.3	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38033**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38033	O-MIC-WIND-240724/3897
Out-of-bounds Write	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38025**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38025	O-MIC-WIND-240724/3898
Out-of-bounds Read	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38028**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38028	O-MIC-WIND-240724/3899
Integer Overflow or Wraparound	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38019	O-MIC-WIND-240724/3900

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
			CVE ID: CVE-2024-38019		
N/A	09-Jul-2024	7.1	Windows NTLM Spoofing Vulnerability **CVE ID: CVE-2024-30081**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30081	O-MIC-WIND-240724/3901
Improper Link Resolution Before File Access ('Link Following')	09-Jul-2024	7	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38022**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38022	O-MIC-WIND-240724/3902
Improper Verification of Cryptographic Signature	09-Jul-2024	7	Windows Enroll Engine Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38069**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38069	O-MIC-WIND-240724/3903
N/A	09-Jul-2024	6.8	BitLocker Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38058**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38058	O-MIC-WIND-240724/3904
Out-of-bounds Write	09-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38065**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38065	O-MIC-WIND-240724/3905
N/A	09-Jul-2024	6.7	Microsoft Windows Server Backup Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38013	O-MIC-WIND-240724/3906

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-Jul-2024	6.5	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability **CVE ID: CVE-2024-38048**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38048	O-MIC-WIND-240724/3907
N/A	09-Jul-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID: CVE-2024-38030**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38030	O-MIC-WIND-240724/3908
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38101**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38101	O-MIC-WIND-240724/3909
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38102**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38102	O-MIC-WIND-240724/3910
N/A	09-Jul-2024	6.5	Windows Line Printer Daemon Service Denial of Service Vulnerability **CVE ID: CVE-2024-38027**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38027	O-MIC-WIND-240724/3911
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38105	O-MIC-WIND-240724/3912

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38105		
N/A	09-Jul-2024	5.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID: CVE-2024-38017**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38017	O-MIC-WIND-240724/3913
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38055	O-MIC-WIND-240724/3914
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38056	O-MIC-WIND-240724/3915
N/A	09-Jul-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38041**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38041	O-MIC-WIND-240724/3916
N/A	09-Jul-2024	5.3	Windows iSCSI Service Denial of Service Vulnerability **CVE ID: CVE-2024-35270**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35270	O-MIC-WIND-240724/3917
N/A	09-Jul-2024	4.7	Windows Remote Access Connection Manager Information	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/3918

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-30071**	lity/CVE-2024-30071	
Product: windows_10_1809					
Affected Version(s): * Up to (excluding) 10.0.17763.6054					
N/A	09-Jul-2024	8.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-28899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28899	O-MIC-WIND-240724/3919
N/A	09-Jul-2024	8.8	Windows MultiPoint Services Remote Code Execution Vulnerability **CVE ID: CVE-2024-30013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30013	O-MIC-WIND-240724/3920
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jul-2024	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38104**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38104	O-MIC-WIND-240724/3921
Out-of-bounds Write	09-Jul-2024	8.8	Windows Imaging Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38060**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38060	O-MIC-WIND-240724/3922
Use After Free	09-Jul-2024	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38053	O-MIC-WIND-240724/3923

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38053		
N/A	09-Jul-2024	8.4	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37984	O-MIC-WIND-240724/3924
Externally Controlled Reference to a Resource in Another Sphere	09-Jul-2024	8.1	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability **CVE ID: CVE-2024-38049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38049	O-MIC-WIND-240724/3925
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38010**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38010	O-MIC-WIND-240724/3926
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38011**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38011	O-MIC-WIND-240724/3927
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37969**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37969	O-MIC-WIND-240724/3928
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/3929

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-37970	lity/CVE-2024-37970	
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37971**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37971	O-MIC-WIND-240724/3930
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37972**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37972	O-MIC-WIND-240724/3931
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37974**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37974	O-MIC-WIND-240724/3932
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37975**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37975	O-MIC-WIND-240724/3933
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37981**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37981	O-MIC-WIND-240724/3934
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37986**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37986	O-MIC-WIND-240724/3935

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37987**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37987	O-MIC-WIND-240724/3936
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37988**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37988	O-MIC-WIND-240724/3937
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37989**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37989	O-MIC-WIND-240724/3938
Integer Underflow (Wrap or Wraparound)	09-Jul-2024	7.8	Windows Workstation Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38050**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38050	O-MIC-WIND-240724/3939
N/A	09-Jul-2024	7.8	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability **CVE ID: CVE-2024-30079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30079	O-MIC-WIND-240724/3940
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38052	O-MIC-WIND-240724/3941

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38054	O-MIC-WIND-240724/3942
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38057	O-MIC-WIND-240724/3943
N/A	09-Jul-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37973**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37973	O-MIC-WIND-240724/3944
N/A	09-Jul-2024	7.8	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38070**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38070	O-MIC-WIND-240724/3945
N/A	09-Jul-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38062	O-MIC-WIND-240724/3946
N/A	09-Jul-2024	7.8	Windows Filtering Platform Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/3947

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
			CVE ID: CVE-2024-38034	lity/CVE-2024-38034	
Use After Free	09-Jul-2024	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38066**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38066	O-MIC-WIND-240724/3948
N/A	09-Jul-2024	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38079	O-MIC-WIND-240724/3949
Out-of-bounds Write	09-Jul-2024	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38051**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38051	O-MIC-WIND-240724/3950
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38043	O-MIC-WIND-240724/3951
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38047**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38047	O-MIC-WIND-240724/3952
N/A	09-Jul-2024	7.5	Windows Cryptographic Services Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30098	O-MIC-WIND-240724/3953

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-30098		
N/A	09-Jul-2024	7.5	Windows TCP/IP Information Disclosure Vulnerability **CVE ID: CVE-2024-38064**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38064	O-MIC-WIND-240724/3954
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38068**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38068	O-MIC-WIND-240724/3955
N/A	09-Jul-2024	7.5	DCOM Remote Cross-Session Activation Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38061	O-MIC-WIND-240724/3956
N/A	09-Jul-2024	7.5	Microsoft WS-Discovery Denial of Service Vulnerability **CVE ID: CVE-2024-38091**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38091	O-MIC-WIND-240724/3957
User Interface (UI) Misrepresentation of Critical Information	09-Jul-2024	7.5	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-38112**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112	O-MIC-WIND-240724/3958
N/A	09-Jul-2024	7.3	PowerShell Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/3959

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38033**	guide/vulnerability/CVE-2024-38033	
Out-of-bounds Write	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38025**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38025	O-MIC-WIND-240724/3960
Out-of-bounds Read	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38028**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38028	O-MIC-WIND-240724/3961
Integer Overflow or Wraparound	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38019**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38019	O-MIC-WIND-240724/3962
N/A	09-Jul-2024	7.1	Windows NTLM Spoofing Vulnerability **CVE ID: CVE-2024-30081**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30081	O-MIC-WIND-240724/3963
Improper Link Resolution Before File Access ('Link Following')	09-Jul-2024	7	Windows Image Acquisition Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38022	O-MIC-WIND-240724/3964

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38022		
Improper Verification of Cryptographic Signature	09-Jul-2024	7	Windows Enroll Engine Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38069**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38069	O-MIC-WIND-240724/3965
N/A	09-Jul-2024	6.8	BitLocker Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38058**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38058	O-MIC-WIND-240724/3966
Out-of-bounds Write	09-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38065**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38065	O-MIC-WIND-240724/3967
N/A	09-Jul-2024	6.7	Microsoft Windows Server Backup Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38013	O-MIC-WIND-240724/3968
Out-of-bounds Read	09-Jul-2024	6.5	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability **CVE ID: CVE-2024-38048**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38048	O-MIC-WIND-240724/3969
N/A	09-Jul-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID: CVE-2024-38030**	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/3970

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lity/CVE-2024-38030	
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38101**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38101	O-MIC-WIND-240724/3971
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38102**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38102	O-MIC-WIND-240724/3972
N/A	09-Jul-2024	6.5	Windows Line Printer Daemon Service Denial of Service Vulnerability **CVE ID: CVE-2024-38027**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38027	O-MIC-WIND-240724/3973
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38105**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38105	O-MIC-WIND-240724/3974
N/A	09-Jul-2024	5.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID: CVE-2024-38017**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38017	O-MIC-WIND-240724/3975
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/3976

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38055**	guide/vulnerability/CVE-2024-38055	
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38056	O-MIC-WIND-240724/3977
N/A	09-Jul-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38041**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38041	O-MIC-WIND-240724/3978
N/A	09-Jul-2024	5.3	Windows iSCSI Service Denial of Service Vulnerability **CVE ID: CVE-2024-35270**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35270	O-MIC-WIND-240724/3979
N/A	09-Jul-2024	4.7	Windows Remote Access Connection Manager Information Disclosure Vulnerability **CVE ID: CVE-2024-30071**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30071	O-MIC-WIND-240724/3980
Product: windows_10_21h2					
Affected Version(s): * Up to (excluding) 10.0.19044.4651					
Improper Restriction of Operations within the Bounds of a	09-Jul-2024	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38104**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38104	O-MIC-WIND-240724/3981

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Buffer					
N/A	09-Jul-2024	8.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-28899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28899	O-MIC-WIND-240724/3982
N/A	09-Jul-2024	8.8	Windows MultiPoint Services Remote Code Execution Vulnerability **CVE ID: CVE-2024-30013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30013	O-MIC-WIND-240724/3983
Out-of-bounds Write	09-Jul-2024	8.8	Windows Imaging Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38060**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38060	O-MIC-WIND-240724/3984
Use After Free	09-Jul-2024	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability **CVE ID: CVE-2024-38053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38053	O-MIC-WIND-240724/3985
N/A	09-Jul-2024	8.4	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37984	O-MIC-WIND-240724/3986
Externally Controlled Reference to a Resource	09-Jul-2024	8.1	Windows Distributed Transaction Coordinator Remote Code	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/3987

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Another Sphere			Execution Vulnerability **CVE ID: CVE-2024-38049**	lity/CVE-2024-38049	
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37969**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37969	O-MIC-WIND-240724/3988
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37970**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37970	O-MIC-WIND-240724/3989
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37971**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37971	O-MIC-WIND-240724/3990
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37972**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37972	O-MIC-WIND-240724/3991
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37974**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37974	O-MIC-WIND-240724/3992
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37975	O-MIC-WIND-240724/3993

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-37975		
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37981**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37981	O-MIC-WIND-240724/3994
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37987**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37987	O-MIC-WIND-240724/3995
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37988**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37988	O-MIC-WIND-240724/3996
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37989**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37989	O-MIC-WIND-240724/3997
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38010**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38010	O-MIC-WIND-240724/3998
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38011**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38011	O-MIC-WIND-240724/3999

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37986**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37986	O-MIC-WIND-240724/4000
N/A	09-Jul-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38062	O-MIC-WIND-240724/4001
N/A	09-Jul-2024	7.8	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability **CVE ID: CVE-2024-30079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30079	O-MIC-WIND-240724/4002
N/A	09-Jul-2024	7.8	Windows Filtering Platform Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38034	O-MIC-WIND-240724/4003
N/A	09-Jul-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38059**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38059	O-MIC-WIND-240724/4004
N/A	09-Jul-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37973**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37973	O-MIC-WIND-240724/4005

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38054	O-MIC-WIND-240724/4006
Out-of-bounds Write	09-Jul-2024	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38051**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38051	O-MIC-WIND-240724/4007
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38057	O-MIC-WIND-240724/4008
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38052	O-MIC-WIND-240724/4009
Integer Underflow (Wrap or Wraparound)	09-Jul-2024	7.8	Windows Workstation Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38050**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38050	O-MIC-WIND-240724/4010
N/A	09-Jul-2024	7.8	PowerShell Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/4011

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
			Privilege Vulnerability **CVE ID: CVE-2024-38047**	guide/vulnerability/CVE-2024-38047	
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38043	O-MIC-WIND-240724/4012
Use After Free	09-Jul-2024	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38066**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38066	O-MIC-WIND-240724/4013
N/A	09-Jul-2024	7.8	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38070**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38070	O-MIC-WIND-240724/4014
N/A	09-Jul-2024	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38079	O-MIC-WIND-240724/4015
N/A	09-Jul-2024	7.5	Windows Cryptographic Services Security Feature Bypass Vulnerability **CVE ID: CVE-2024-30098**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30098	O-MIC-WIND-240724/4016
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP)	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/4017

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Denial of Service Vulnerability **CVE ID: CVE-2024-38068**	guide/vulnerability/CVE-2024-38068	
User Interface (UI) Misrepresentation of Critical Information	09-Jul-2024	7.5	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-38112**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112	O-MIC-WIND-240724/4018
N/A	09-Jul-2024	7.5	DCOM Remote Cross-Session Activation Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38061	O-MIC-WIND-240724/4019
N/A	09-Jul-2024	7.5	Microsoft WS-Discovery Denial of Service Vulnerability **CVE ID: CVE-2024-38091**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38091	O-MIC-WIND-240724/4020
N/A	09-Jul-2024	7.5	Windows TCP/IP Information Disclosure Vulnerability **CVE ID: CVE-2024-38064**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38064	O-MIC-WIND-240724/4021
N/A	09-Jul-2024	7.3	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38033**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38033	O-MIC-WIND-240724/4022

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
Integer Overflow or Wraparound	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38019**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38019	O-MIC-WIND-240724/4023
Out-of-bounds Read	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38028**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38028	O-MIC-WIND-240724/4024
Out-of-bounds Write	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38025**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38025	O-MIC-WIND-240724/4025
N/A	09-Jul-2024	7.1	Windows NTLM Spoofing Vulnerability **CVE ID: CVE-2024-30081**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30081	O-MIC-WIND-240724/4026
Out-of-bounds Write	09-Jul-2024	7.1	Microsoft Xbox Remote Code Execution Vulnerability **CVE ID: CVE-2024-38032**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38032	O-MIC-WIND-240724/4027
Improper Link Resolution Before File Access	09-Jul-2024	7	Windows Image Acquisition Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4028

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Link Following')			**CVE ID: CVE-2024-38022**	lity/CVE-2024-38022	
Improper Verification of Cryptographic Signature	09-Jul-2024	7	Windows Enroll Engine Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38069**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38069	O-MIC-WIND-240724/4029
N/A	09-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-26184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26184	O-MIC-WIND-240724/4030
N/A	09-Jul-2024	6.8	BitLocker Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38058**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38058	O-MIC-WIND-240724/4031
Out-of-bounds Write	09-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38065**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38065	O-MIC-WIND-240724/4032
N/A	09-Jul-2024	6.7	Microsoft Windows Server Backup Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38013	O-MIC-WIND-240724/4033
N/A	09-Jul-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID: CVE-2024-38030**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38030	O-MIC-WIND-240724/4034

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-Jul-2024	6.5	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability **CVE ID: CVE-2024-38048**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38048	O-MIC-WIND-240724/4035
N/A	09-Jul-2024	6.5	Windows Line Printer Daemon Service Denial of Service Vulnerability **CVE ID: CVE-2024-38027**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38027	O-MIC-WIND-240724/4036
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38101**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38101	O-MIC-WIND-240724/4037
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38102**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38102	O-MIC-WIND-240724/4038
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38105**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38105	O-MIC-WIND-240724/4039
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4040

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38055**	lity/CVE-2024-38055	
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38056	O-MIC-WIND-240724/4041
N/A	09-Jul-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38041**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38041	O-MIC-WIND-240724/4042
N/A	09-Jul-2024	5.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID: CVE-2024-38017**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38017	O-MIC-WIND-240724/4043
N/A	09-Jul-2024	5.3	Windows iSCSI Service Denial of Service Vulnerability **CVE ID: CVE-2024-35270**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35270	O-MIC-WIND-240724/4044
N/A	09-Jul-2024	4.7	Windows Remote Access Connection Manager Information Disclosure Vulnerability **CVE ID: CVE-2024-30071**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30071	O-MIC-WIND-240724/4045
Product: windows_10_22h2					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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) 10.0.19045.4651					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jul-2024	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38104**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38104	O-MIC-WIND-240724/4046
N/A	09-Jul-2024	8.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-28899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28899	O-MIC-WIND-240724/4047
N/A	09-Jul-2024	8.8	Windows MultiPoint Services Remote Code Execution Vulnerability **CVE ID: CVE-2024-30013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30013	O-MIC-WIND-240724/4048
Out-of-bounds Write	09-Jul-2024	8.8	Windows Imaging Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38060**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38060	O-MIC-WIND-240724/4049
Use After Free	09-Jul-2024	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability **CVE ID: CVE-2024-38053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38053	O-MIC-WIND-240724/4050
N/A	09-Jul-2024	8.4	Secure Boot Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4051

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-37984	lity/CVE-2024-37984	
Externally Controlled Reference to a Resource in Another Sphere	09-Jul-2024	8.1	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability **CVE ID: CVE-2024-38049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38049	O-MIC-WIND-240724/4052
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37969**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37969	O-MIC-WIND-240724/4053
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37970**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37970	O-MIC-WIND-240724/4054
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37971**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37971	O-MIC-WIND-240724/4055
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37972**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37972	O-MIC-WIND-240724/4056
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-37974	lity/CVE-2024-37974	
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37975**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37975	O-MIC-WIND-240724/4058
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37981**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37981	O-MIC-WIND-240724/4059
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37987**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37987	O-MIC-WIND-240724/4060
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37988**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37988	O-MIC-WIND-240724/4061
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37989**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37989	O-MIC-WIND-240724/4062
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38010**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38010	O-MIC-WIND-240724/4063

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38011**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38011	O-MIC-WIND-240724/4064
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37986**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37986	O-MIC-WIND-240724/4065
N/A	09-Jul-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38062	O-MIC-WIND-240724/4066
N/A	09-Jul-2024	7.8	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability **CVE ID: CVE-2024-30079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30079	O-MIC-WIND-240724/4067
N/A	09-Jul-2024	7.8	Windows Filtering Platform Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38034	O-MIC-WIND-240724/4068
N/A	09-Jul-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38059**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38059	O-MIC-WIND-240724/4069
N/A	09-Jul-2024	7.8	Secure Boot Security Feature	https://msrc.microsoft.com/up	O-MIC-WIND-240724/4070

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bypass Vulnerability **CVE ID: CVE-2024-37973**	date-guide/vulnerability/CVE-2024-37973	
Out-of-bounds Write	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38054	O-MIC-WIND-240724/4071
Out-of-bounds Write	09-Jul-2024	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38051**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38051	O-MIC-WIND-240724/4072
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38057	O-MIC-WIND-240724/4073
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38052	O-MIC-WIND-240724/4074
Integer Underflow (Wrap or Wraparound)	09-Jul-2024	7.8	Windows Workstation Service Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4075

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38050	lity/CVE-2024-38050	
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38047**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38047	O-MIC-WIND-240724/4076
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38043	O-MIC-WIND-240724/4077
Use After Free	09-Jul-2024	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38066**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38066	O-MIC-WIND-240724/4078
N/A	09-Jul-2024	7.8	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38070**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38070	O-MIC-WIND-240724/4079
N/A	09-Jul-2024	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38079	O-MIC-WIND-240724/4080
N/A	09-Jul-2024	7.5	Windows Cryptographic Services Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30098	O-MIC-WIND-240724/4081

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-30098		
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38068**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38068	O-MIC-WIND-240724/4082
User Interface (UI) Misrepresentation of Critical Information	09-Jul-2024	7.5	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-38112**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112	O-MIC-WIND-240724/4083
N/A	09-Jul-2024	7.5	DCOM Remote Cross-Session Activation Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38061	O-MIC-WIND-240724/4084
N/A	09-Jul-2024	7.5	Microsoft WS-Discovery Denial of Service Vulnerability **CVE ID: CVE-2024-38091**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38091	O-MIC-WIND-240724/4085
N/A	09-Jul-2024	7.5	Windows TCP/IP Information Disclosure Vulnerability **CVE ID: CVE-2024-38064**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38064	O-MIC-WIND-240724/4086
N/A	09-Jul-2024	7.3	PowerShell Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/4087

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38033**	guide/vulnerability/CVE-2024-38033	
Integer Overflow or Wraparound	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38019**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38019	O-MIC-WIND-240724/4088
Out-of-bounds Read	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38028**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38028	O-MIC-WIND-240724/4089
Out-of-bounds Write	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38025**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38025	O-MIC-WIND-240724/4090
N/A	09-Jul-2024	7.1	Windows NTLM Spoofing Vulnerability **CVE ID: CVE-2024-30081**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30081	O-MIC-WIND-240724/4091
Out-of-bounds Write	09-Jul-2024	7.1	Microsoft Xbox Remote Code Execution Vulnerability **CVE ID: CVE-2024-38032**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38032	O-MIC-WIND-240724/4092

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Link Resolution Before File Access ('Link Following')	09-Jul-2024	7	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38022**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38022	O-MIC-WIND-240724/4093
Improper Verification of Cryptographic Signature	09-Jul-2024	7	Windows Enroll Engine Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38069**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38069	O-MIC-WIND-240724/4094
N/A	09-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-26184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26184	O-MIC-WIND-240724/4095
N/A	09-Jul-2024	6.8	BitLocker Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38058**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38058	O-MIC-WIND-240724/4096
Out-of-bounds Write	09-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38065**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38065	O-MIC-WIND-240724/4097
N/A	09-Jul-2024	6.7	Microsoft Windows Server Backup Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38013	O-MIC-WIND-240724/4098

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID: CVE-2024-38030**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38030	O-MIC-WIND-240724/4099
Out-of-bounds Read	09-Jul-2024	6.5	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability **CVE ID: CVE-2024-38048**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38048	O-MIC-WIND-240724/4100
N/A	09-Jul-2024	6.5	Windows Line Printer Daemon Service Denial of Service Vulnerability **CVE ID: CVE-2024-38027**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38027	O-MIC-WIND-240724/4101
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38101**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38101	O-MIC-WIND-240724/4102
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38102**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38102	O-MIC-WIND-240724/4103
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38105	O-MIC-WIND-240724/4104

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38105		
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38055	O-MIC-WIND-240724/4105
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38056	O-MIC-WIND-240724/4106
N/A	09-Jul-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38041**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38041	O-MIC-WIND-240724/4107
N/A	09-Jul-2024	5.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID: CVE-2024-38017**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38017	O-MIC-WIND-240724/4108
N/A	09-Jul-2024	5.3	Windows iSCSI Service Denial of Service Vulnerability **CVE ID: CVE-2024-35270**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35270	O-MIC-WIND-240724/4109
N/A	09-Jul-2024	4.7	Windows Remote Access Connection Manager Information	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4110

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-30071**	lity/CVE-2024-30071	
Product: windows_11_21h2					
Affected Version(s): * Up to (excluding) 10.0.22000.3079					
N/A	09-Jul-2024	8.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-28899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28899	O-MIC-WIND-240724/4111
N/A	09-Jul-2024	8.8	Windows MultiPoint Services Remote Code Execution Vulnerability **CVE ID: CVE-2024-30013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30013	O-MIC-WIND-240724/4112
Use After Free	09-Jul-2024	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability **CVE ID: CVE-2024-38053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38053	O-MIC-WIND-240724/4113
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jul-2024	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38104**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38104	O-MIC-WIND-240724/4114
Out-of-bounds Write	09-Jul-2024	8.8	Windows Imaging Component Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38060	O-MIC-WIND-240724/4115

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38060		
N/A	09-Jul-2024	8.4	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37984	O-MIC-WIND-240724/4116
Externally Controlled Reference to a Resource in Another Sphere	09-Jul-2024	8.1	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability **CVE ID: CVE-2024-38049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38049	O-MIC-WIND-240724/4117
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37969**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37969	O-MIC-WIND-240724/4118
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37989**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37989	O-MIC-WIND-240724/4119
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38010**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38010	O-MIC-WIND-240724/4120
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4121

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38011	lity/CVE-2024-38011	
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37981**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37981	O-MIC-WIND-240724/4122
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37970**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37970	O-MIC-WIND-240724/4123
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37971**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37971	O-MIC-WIND-240724/4124
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37972**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37972	O-MIC-WIND-240724/4125
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37974**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37974	O-MIC-WIND-240724/4126
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37975**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37975	O-MIC-WIND-240724/4127

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37977**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37977	O-MIC-WIND-240724/4128
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37986**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37986	O-MIC-WIND-240724/4129
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37987**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37987	O-MIC-WIND-240724/4130
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37988**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37988	O-MIC-WIND-240724/4131
Integer Underflow (Wrap or Wraparound)	09-Jul-2024	7.8	Windows Workstation Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38050**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38050	O-MIC-WIND-240724/4132
N/A	09-Jul-2024	7.8	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability **CVE ID: CVE-2024-30079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30079	O-MIC-WIND-240724/4133

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
Out-of-bounds Write	09-Jul-2024	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38051**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38051	O-MIC-WIND-240724/4134
Out-of-bounds Write	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38054	O-MIC-WIND-240724/4135
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38057	O-MIC-WIND-240724/4136
N/A	09-Jul-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37973**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37973	O-MIC-WIND-240724/4137
N/A	09-Jul-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38059**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38059	O-MIC-WIND-240724/4138
N/A	09-Jul-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38062	O-MIC-WIND-240724/4139

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38062		
Use After Free	09-Jul-2024	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38066**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38066	O-MIC-WIND-240724/4140
N/A	09-Jul-2024	7.8	Windows Filtering Platform Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38034	O-MIC-WIND-240724/4141
N/A	09-Jul-2024	7.8	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38070**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38070	O-MIC-WIND-240724/4142
N/A	09-Jul-2024	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38079	O-MIC-WIND-240724/4143
N/A	09-Jul-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38080**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38080	O-MIC-WIND-240724/4144
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38052	O-MIC-WIND-240724/4145

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38052		
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38043	O-MIC-WIND-240724/4146
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38047**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38047	O-MIC-WIND-240724/4147
N/A	09-Jul-2024	7.5	Windows Cryptographic Services Security Feature Bypass Vulnerability **CVE ID: CVE-2024-30098**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30098	O-MIC-WIND-240724/4148
N/A	09-Jul-2024	7.5	DCOM Remote Cross-Session Activation Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38061	O-MIC-WIND-240724/4149
N/A	09-Jul-2024	7.5	Windows TCP/IP Information Disclosure Vulnerability **CVE ID: CVE-2024-38064**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38064	O-MIC-WIND-240724/4150
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4151

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
			Service Vulnerability **CVE ID: CVE-2024-38068**	lity/CVE-2024-38068	
N/A	09-Jul-2024	7.5	Xbox Wireless Adapter Remote Code Execution Vulnerability **CVE ID: CVE-2024-38078**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38078	O-MIC-WIND-240724/4152
N/A	09-Jul-2024	7.5	Microsoft WS-Discovery Denial of Service Vulnerability **CVE ID: CVE-2024-38091**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38091	O-MIC-WIND-240724/4153
User Interface (UI) Misrepresentation of Critical Information	09-Jul-2024	7.5	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-38112**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112	O-MIC-WIND-240724/4154
N/A	09-Jul-2024	7.3	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38033**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38033	O-MIC-WIND-240724/4155
Out-of-bounds Write	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38025**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38025	O-MIC-WIND-240724/4156
Integer Overflow	09-Jul-2024	7.2	Microsoft Windows Performance Data	https://msrc.microsoft.com/up	O-MIC-WIND-240724/4157

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Wraparound			Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38019**	date-guide/vulnerability/CVE-2024-38019	
Out-of-bounds Read	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38028**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38028	O-MIC-WIND-240724/4158
N/A	09-Jul-2024	7.1	Windows NTLM Spoofing Vulnerability **CVE ID: CVE-2024-30081**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30081	O-MIC-WIND-240724/4159
Out-of-bounds Write	09-Jul-2024	7.1	Microsoft Xbox Remote Code Execution Vulnerability **CVE ID: CVE-2024-38032**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38032	O-MIC-WIND-240724/4160
Improper Link Resolution Before File Access ('Link Following')	09-Jul-2024	7	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38022**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38022	O-MIC-WIND-240724/4161
Improper Verification of Cryptographic Signature	09-Jul-2024	7	Windows Enroll Engine Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38069**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38069	O-MIC-WIND-240724/4162

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-26184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26184	O-MIC-WIND-240724/4163
N/A	09-Jul-2024	6.8	BitLocker Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38058**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38058	O-MIC-WIND-240724/4164
Out-of-bounds Write	09-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38065**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38065	O-MIC-WIND-240724/4165
N/A	09-Jul-2024	6.7	Microsoft Windows Server Backup Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38013	O-MIC-WIND-240724/4166
N/A	09-Jul-2024	6.5	Windows Line Printer Daemon Service Denial of Service Vulnerability **CVE ID: CVE-2024-38027**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38027	O-MIC-WIND-240724/4167
Out-of-bounds Read	09-Jul-2024	6.5	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability **CVE ID: CVE-2024-38048**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38048	O-MIC-WIND-240724/4168

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID: CVE-2024-38030**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38030	O-MIC-WIND-240724/4169
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38101**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38101	O-MIC-WIND-240724/4170
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38102**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38102	O-MIC-WIND-240724/4171
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38105**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38105	O-MIC-WIND-240724/4172
N/A	09-Jul-2024	5.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID: CVE-2024-38017**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38017	O-MIC-WIND-240724/4173
N/A	09-Jul-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38041**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38041	O-MIC-WIND-240724/4174

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38055	O-MIC-WIND-240724/4175
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38056	O-MIC-WIND-240724/4176
N/A	09-Jul-2024	5.3	Windows iSCSI Service Denial of Service Vulnerability **CVE ID: CVE-2024-35270**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35270	O-MIC-WIND-240724/4177
N/A	09-Jul-2024	4.7	Windows Remote Access Connection Manager Information Disclosure Vulnerability **CVE ID: CVE-2024-30071**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30071	O-MIC-WIND-240724/4178
Product: windows_11_22h2					
Affected Version(s): * Up to (excluding) 10.0.22621.3880					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jul-2024	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38104**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38104	O-MIC-WIND-240724/4179
N/A	09-Jul-2024	8.8	Secure Boot Security Feature	https://msrc.microsoft.com/up	O-MIC-WIND-240724/4180

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bypass Vulnerability **CVE ID: CVE-2024-28899**	date-guide/vulnerability/CVE-2024-28899	
N/A	09-Jul-2024	8.8	Windows MultiPoint Services Remote Code Execution Vulnerability **CVE ID: CVE-2024-30013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30013	O-MIC-WIND-240724/4181
Use After Free	09-Jul-2024	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability **CVE ID: CVE-2024-38053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38053	O-MIC-WIND-240724/4182
Out-of-bounds Write	09-Jul-2024	8.8	Windows Imaging Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38060**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38060	O-MIC-WIND-240724/4183
N/A	09-Jul-2024	8.4	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37984	O-MIC-WIND-240724/4184
Externally Controlled Reference to a Resource in Another Sphere	09-Jul-2024	8.1	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability **CVE ID: CVE-2024-38049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38049	O-MIC-WIND-240724/4185

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37989**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37989	O-MIC-WIND-240724/4186
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38010**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38010	O-MIC-WIND-240724/4187
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38011**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38011	O-MIC-WIND-240724/4188
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37986**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37986	O-MIC-WIND-240724/4189
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37978**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37978	O-MIC-WIND-240724/4190
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37970**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37970	O-MIC-WIND-240724/4191
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4192

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-37971	lity/CVE-2024-37971	
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37972**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37972	O-MIC-WIND-240724/4193
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37974**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37974	O-MIC-WIND-240724/4194
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37975**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37975	O-MIC-WIND-240724/4195
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37977**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37977	O-MIC-WIND-240724/4196
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37981**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37981	O-MIC-WIND-240724/4197
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37969**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37969	O-MIC-WIND-240724/4198

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37987**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37987	O-MIC-WIND-240724/4199
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37988**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37988	O-MIC-WIND-240724/4200
N/A	09-Jul-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38062	O-MIC-WIND-240724/4201
N/A	09-Jul-2024	7.8	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability **CVE ID: CVE-2024-30079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30079	O-MIC-WIND-240724/4202
N/A	09-Jul-2024	7.8	Windows Filtering Platform Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38034	O-MIC-WIND-240724/4203
N/A	09-Jul-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38059**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38059	O-MIC-WIND-240724/4204

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-Jul-2024	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38051**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38051	O-MIC-WIND-240724/4205
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38057	O-MIC-WIND-240724/4206
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38052	O-MIC-WIND-240724/4207
Integer Underflow (Wrap or Wraparound)	09-Jul-2024	7.8	Windows Workstation Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38050**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38050	O-MIC-WIND-240724/4208
N/A	09-Jul-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37973**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37973	O-MIC-WIND-240724/4209
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4210

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38047	lity/CVE-2024-38047	
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38043	O-MIC-WIND-240724/4211
Use After Free	09-Jul-2024	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38066**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38066	O-MIC-WIND-240724/4212
N/A	09-Jul-2024	7.8	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38070**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38070	O-MIC-WIND-240724/4213
N/A	09-Jul-2024	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38079	O-MIC-WIND-240724/4214
N/A	09-Jul-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38080**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38080	O-MIC-WIND-240724/4215
Out-of-bounds Write	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38054	O-MIC-WIND-240724/4216

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38054		
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38068**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38068	O-MIC-WIND-240724/4217
N/A	09-Jul-2024	7.5	Xbox Wireless Adapter Remote Code Execution Vulnerability **CVE ID: CVE-2024-38078**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38078	O-MIC-WIND-240724/4218
N/A	09-Jul-2024	7.5	DCOM Remote Cross-Session Activation Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38061	O-MIC-WIND-240724/4219
N/A	09-Jul-2024	7.5	Windows TCP/IP Information Disclosure Vulnerability **CVE ID: CVE-2024-38064**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38064	O-MIC-WIND-240724/4220
N/A	09-Jul-2024	7.5	Microsoft WS-Discovery Denial of Service Vulnerability **CVE ID: CVE-2024-38091**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38091	O-MIC-WIND-240724/4221
N/A	09-Jul-2024	7.5	Windows Cryptographic Services Security	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4222

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Feature Bypass Vulnerability **CVE ID: CVE-2024-30098**	lity/CVE-2024-30098	
User Interface (UI) Misrepresentation of Critical Information	09-Jul-2024	7.5	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-38112**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112	O-MIC-WIND-240724/4223
N/A	09-Jul-2024	7.3	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38033**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38033	O-MIC-WIND-240724/4224
Out-of-bounds Read	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38028**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38028	O-MIC-WIND-240724/4225
Out-of-bounds Write	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38025**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38025	O-MIC-WIND-240724/4226
Integer Overflow or Wraparound	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38019	O-MIC-WIND-240724/4227

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38019		
N/A	09-Jul-2024	7.1	Windows NTLM Spoofing Vulnerability **CVE ID: CVE-2024-30081**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30081	O-MIC-WIND-240724/4228
Out-of-bounds Write	09-Jul-2024	7.1	Microsoft Xbox Remote Code Execution Vulnerability **CVE ID: CVE-2024-38032**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38032	O-MIC-WIND-240724/4229
Improper Verification of Cryptographic Signature	09-Jul-2024	7	Windows Enroll Engine Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38069**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38069	O-MIC-WIND-240724/4230
Improper Link Resolution Before File Access ('Link Following')	09-Jul-2024	7	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38022**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38022	O-MIC-WIND-240724/4231
N/A	09-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-26184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26184	O-MIC-WIND-240724/4232
N/A	09-Jul-2024	6.8	BitLocker Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38058**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38058	O-MIC-WIND-240724/4233

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38065**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38065	O-MIC-WIND-240724/4234
N/A	09-Jul-2024	6.7	Microsoft Windows Server Backup Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38013	O-MIC-WIND-240724/4235
N/A	09-Jul-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID: CVE-2024-38030**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38030	O-MIC-WIND-240724/4236
Out-of-bounds Read	09-Jul-2024	6.5	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability **CVE ID: CVE-2024-38048**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38048	O-MIC-WIND-240724/4237
N/A	09-Jul-2024	6.5	Windows Line Printer Daemon Service Denial of Service Vulnerability **CVE ID: CVE-2024-38027**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38027	O-MIC-WIND-240724/4238
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38101	O-MIC-WIND-240724/4239

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-2024-38101		
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38102**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38102	O-MIC-WIND-240724/4240
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38105**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38105	O-MIC-WIND-240724/4241
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38055	O-MIC-WIND-240724/4242
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38056	O-MIC-WIND-240724/4243
N/A	09-Jul-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38041**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38041	O-MIC-WIND-240724/4244
N/A	09-Jul-2024	5.5	Microsoft Message Queuing Information	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4245

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38017**	lity/CVE-2024-38017	
N/A	09-Jul-2024	5.3	Windows iSCSI Service Denial of Service Vulnerability **CVE ID: CVE-2024-35270**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35270	O-MIC-WIND-240724/4246
N/A	09-Jul-2024	4.7	Windows Remote Access Connection Manager Information Disclosure Vulnerability **CVE ID: CVE-2024-30071**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30071	O-MIC-WIND-240724/4247
Product: windows_11_23h2					
Affected Version(s): * Up to (excluding) 10.0.22631.3880					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jul-2024	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38104**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38104	O-MIC-WIND-240724/4248
N/A	09-Jul-2024	8.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-28899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28899	O-MIC-WIND-240724/4249
N/A	09-Jul-2024	8.8	Windows MultiPoint Services Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30013	O-MIC-WIND-240724/4250

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-30013		
Use After Free	09-Jul-2024	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability **CVE ID: CVE-2024-38053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38053	O-MIC-WIND-240724/4251
Out-of-bounds Write	09-Jul-2024	8.8	Windows Imaging Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38060**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38060	O-MIC-WIND-240724/4252
N/A	09-Jul-2024	8.4	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37984	O-MIC-WIND-240724/4253
Externally Controlled Reference to a Resource in Another Sphere	09-Jul-2024	8.1	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability **CVE ID: CVE-2024-38049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38049	O-MIC-WIND-240724/4254
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37989**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37989	O-MIC-WIND-240724/4255
N/A	09-Jul-2024	8	Secure Boot Security Feature	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/4256

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bypass Vulnerability **CVE ID: CVE-2024-38010**	guide/vulnerability/CVE-2024-38010	
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38011**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38011	O-MIC-WIND-240724/4257
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37986**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37986	O-MIC-WIND-240724/4258
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37978**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37978	O-MIC-WIND-240724/4259
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37970**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37970	O-MIC-WIND-240724/4260
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37971**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37971	O-MIC-WIND-240724/4261
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37972	O-MIC-WIND-240724/4262

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-37972		
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37974**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37974	O-MIC-WIND-240724/4263
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37975**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37975	O-MIC-WIND-240724/4264
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37977**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37977	O-MIC-WIND-240724/4265
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37981**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37981	O-MIC-WIND-240724/4266
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37969**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37969	O-MIC-WIND-240724/4267
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37987**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37987	O-MIC-WIND-240724/4268

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
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37988**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37988	O-MIC-WIND-240724/4269
N/A	09-Jul-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38062	O-MIC-WIND-240724/4270
N/A	09-Jul-2024	7.8	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability **CVE ID: CVE-2024-30079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30079	O-MIC-WIND-240724/4271
N/A	09-Jul-2024	7.8	Windows Filtering Platform Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38034	O-MIC-WIND-240724/4272
N/A	09-Jul-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38059**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38059	O-MIC-WIND-240724/4273
Out-of-bounds Write	09-Jul-2024	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38051**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38051	O-MIC-WIND-240724/4274

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38057	O-MIC-WIND-240724/4275
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38052	O-MIC-WIND-240724/4276
Integer Underflow (Wrap or Wraparound)	09-Jul-2024	7.8	Windows Workstation Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38050**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38050	O-MIC-WIND-240724/4277
N/A	09-Jul-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37973**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37973	O-MIC-WIND-240724/4278
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38047**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38047	O-MIC-WIND-240724/4279
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4280

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38043	lity/CVE-2024-38043	
Use After Free	09-Jul-2024	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38066**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38066	O-MIC-WIND-240724/4281
N/A	09-Jul-2024	7.8	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38070**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38070	O-MIC-WIND-240724/4282
N/A	09-Jul-2024	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38079	O-MIC-WIND-240724/4283
N/A	09-Jul-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38080**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38080	O-MIC-WIND-240724/4284
Out-of-bounds Write	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38054	O-MIC-WIND-240724/4285
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4286

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Vulnerability **CVE ID: CVE-2024-38068**	lity/CVE-2024-38068	
N/A	09-Jul-2024	7.5	Xbox Wireless Adapter Remote Code Execution Vulnerability **CVE ID: CVE-2024-38078**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38078	O-MIC-WIND-240724/4287
N/A	09-Jul-2024	7.5	DCOM Remote Cross-Session Activation Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38061	O-MIC-WIND-240724/4288
N/A	09-Jul-2024	7.5	Windows TCP/IP Information Disclosure Vulnerability **CVE ID: CVE-2024-38064**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38064	O-MIC-WIND-240724/4289
N/A	09-Jul-2024	7.5	Microsoft WS-Discovery Denial of Service Vulnerability **CVE ID: CVE-2024-38091**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38091	O-MIC-WIND-240724/4290
N/A	09-Jul-2024	7.5	Windows Cryptographic Services Security Feature Bypass Vulnerability **CVE ID: CVE-2024-30098**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30098	O-MIC-WIND-240724/4291
User Interface (UI)	09-Jul-2024	7.5	Windows MSHTML Platform Spoofing Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/4292

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
Misrepresentation of Critical Information			**CVE ID: CVE-2024-38112**	guide/vulnerability/CVE-2024-38112	
N/A	09-Jul-2024	7.3	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38033**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38033	O-MIC-WIND-240724/4293
Out-of-bounds Read	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38028**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38028	O-MIC-WIND-240724/4294
Out-of-bounds Write	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38025**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38025	O-MIC-WIND-240724/4295
Integer Overflow or Wraparound	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38019**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38019	O-MIC-WIND-240724/4296
N/A	09-Jul-2024	7.1	Windows NTLM Spoofing Vulnerability **CVE ID: CVE-2024-30081**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30081	O-MIC-WIND-240724/4297

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-Jul-2024	7.1	Microsoft Xbox Remote Code Execution Vulnerability **CVE ID: CVE-2024-38032**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38032	O-MIC-WIND-240724/4298
Improper Verification of Cryptographic Signature	09-Jul-2024	7	Windows Enroll Engine Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38069**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38069	O-MIC-WIND-240724/4299
Improper Link Resolution Before File Access ('Link Following')	09-Jul-2024	7	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38022**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38022	O-MIC-WIND-240724/4300
N/A	09-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-26184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26184	O-MIC-WIND-240724/4301
N/A	09-Jul-2024	6.8	BitLocker Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38058**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38058	O-MIC-WIND-240724/4302
Out-of-bounds Write	09-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38065**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38065	O-MIC-WIND-240724/4303
N/A	09-Jul-2024	6.7	Microsoft Windows Server Backup Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/4304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID: CVE-2024-38013**	guide/vulnerability/CVE-2024-38013	
N/A	09-Jul-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID: CVE-2024-38030**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38030	O-MIC-WIND-240724/4305
Out-of-bounds Read	09-Jul-2024	6.5	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability **CVE ID: CVE-2024-38048**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38048	O-MIC-WIND-240724/4306
N/A	09-Jul-2024	6.5	Windows Line Printer Daemon Service Denial of Service Vulnerability **CVE ID: CVE-2024-38027**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38027	O-MIC-WIND-240724/4307
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38101**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38101	O-MIC-WIND-240724/4308
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38102**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38102	O-MIC-WIND-240724/4309

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38105**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38105	O-MIC-WIND-240724/4310
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38055	O-MIC-WIND-240724/4311
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38056	O-MIC-WIND-240724/4312
N/A	09-Jul-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38041**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38041	O-MIC-WIND-240724/4313
N/A	09-Jul-2024	5.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID: CVE-2024-38017**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38017	O-MIC-WIND-240724/4314
N/A	09-Jul-2024	5.3	Windows iSCSI Service Denial of Service Vulnerability **CVE ID: CVE-2024-35270**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35270	O-MIC-WIND-240724/4315

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	4.7	Windows Remote Access Connection Manager Information Disclosure Vulnerability **CVE ID: CVE-2024-30071**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30071	O-MIC-WIND-240724/4316
Product: windows_server_2008					
Affected Version(s): -					
N/A	09-Jul-2024	9.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38077**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38077	O-MIC-WIND-240724/4317
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jul-2024	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38104**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38104	O-MIC-WIND-240724/4318
Externally Controlled Reference to a Resource in Another Sphere	09-Jul-2024	8.1	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability **CVE ID: CVE-2024-38049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38049	O-MIC-WIND-240724/4319
Out-of-bounds Write	09-Jul-2024	7.8	Windows Graphics Component Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38051	O-MIC-WIND-240724/4320

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-2024-38051		
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38052	O-MIC-WIND-240724/4321
Out-of-bounds Write	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38054	O-MIC-WIND-240724/4322
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38057	O-MIC-WIND-240724/4323
Use After Free	09-Jul-2024	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38066**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38066	O-MIC-WIND-240724/4324
N/A	09-Jul-2024	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38079	O-MIC-WIND-240724/4325

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38031**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38031	O-MIC-WIND-240724/4326
N/A	09-Jul-2024	7.5	Windows TCP/IP Information Disclosure Vulnerability **CVE ID: CVE-2024-38064**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38064	O-MIC-WIND-240724/4327
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38067**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38067	O-MIC-WIND-240724/4328
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38068**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38068	O-MIC-WIND-240724/4329
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38071**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38071	O-MIC-WIND-240724/4330
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4331

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Vulnerability **CVE ID: CVE-2024-38073**	lity/CVE-2024-38073	
N/A	09-Jul-2024	7.5	Microsoft WS-Discovery Denial of Service Vulnerability **CVE ID: CVE-2024-38091**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38091	O-MIC-WIND-240724/4332
User Interface (UI) Misrepresentation of Critical Information	09-Jul-2024	7.5	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-38112**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112	O-MIC-WIND-240724/4333
Integer Overflow or Wraparound	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38019**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38019	O-MIC-WIND-240724/4334
Out-of-bounds Write	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38025**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38025	O-MIC-WIND-240724/4335
Out-of-bounds Read	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38028	O-MIC-WIND-240724/4336

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38028		
N/A	09-Jul-2024	7.1	Windows NTLM Spoofing Vulnerability **CVE ID: CVE-2024-30081**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30081	O-MIC-WIND-240724/4337
N/A	09-Jul-2024	6.5	Windows Line Printer Daemon Service Denial of Service Vulnerability **CVE ID: CVE-2024-38027**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38027	O-MIC-WIND-240724/4338
Out-of-bounds Read	09-Jul-2024	6.5	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability **CVE ID: CVE-2024-38048**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38048	O-MIC-WIND-240724/4339
N/A	09-Jul-2024	5.9	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38099**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38099	O-MIC-WIND-240724/4340
N/A	09-Jul-2024	5.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID: CVE-2024-38017**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38017	O-MIC-WIND-240724/4341
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4342

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38055**	lity/CVE-2024-38055	
N/A	09-Jul-2024	5.3	Windows iSCSI Service Denial of Service Vulnerability **CVE ID: CVE-2024-35270**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35270	O-MIC-WIND-240724/4343
Affected Version(s): r2					
N/A	09-Jul-2024	9.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38074**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38074	O-MIC-WIND-240724/4344
N/A	09-Jul-2024	9.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38077**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38077	O-MIC-WIND-240724/4345
Out-of-bounds Write	09-Jul-2024	8.8	Windows Imaging Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38060**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38060	O-MIC-WIND-240724/4346
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jul-2024	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38104**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38104	O-MIC-WIND-240724/4347

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Externally Controlled Reference to a Resource in Another Sphere	09-Jul-2024	8.1	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability **CVE ID: CVE-2024-38049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38049	O-MIC-WIND-240724/4348
N/A	09-Jul-2024	7.8	Windows Filtering Platform Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38034	O-MIC-WIND-240724/4349
Integer Underflow (Wrap or Wraparound)	09-Jul-2024	7.8	Windows Workstation Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38050**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38050	O-MIC-WIND-240724/4350
Out-of-bounds Write	09-Jul-2024	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38051**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38051	O-MIC-WIND-240724/4351
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38052	O-MIC-WIND-240724/4352
Out-of-bounds Write	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4353

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
			Privilege Vulnerability **CVE ID: CVE-2024-38054**	lity/CVE-2024-38054	
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38057	O-MIC-WIND-240724/4354
Use After Free	09-Jul-2024	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38066**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38066	O-MIC-WIND-240724/4355
N/A	09-Jul-2024	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38079	O-MIC-WIND-240724/4356
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38031**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38031	O-MIC-WIND-240724/4357
N/A	09-Jul-2024	7.5	DCOM Remote Cross-Session Activation Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38061	O-MIC-WIND-240724/4358

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38061		
N/A	09-Jul-2024	7.5	Windows TCP/IP Information Disclosure Vulnerability **CVE ID: CVE-2024-38064**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38064	O-MIC-WIND-240724/4359
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38067**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38067	O-MIC-WIND-240724/4360
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38068**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38068	O-MIC-WIND-240724/4361
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38071**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38071	O-MIC-WIND-240724/4362
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38073**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38073	O-MIC-WIND-240724/4363
N/A	09-Jul-2024	7.5	Microsoft WS-Discovery Denial of	https://msrc.microsoft.com/up	O-MIC-WIND-240724/4364

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Vulnerability **CVE ID: CVE-2024-38091**	date-guide/vulnerability/CVE-2024-38091	
Integer Overflow or Wraparound	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38019**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38019	O-MIC-WIND-240724/4365
Out-of-bounds Write	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38025**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38025	O-MIC-WIND-240724/4366
Out-of-bounds Read	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38028**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38028	O-MIC-WIND-240724/4367
N/A	09-Jul-2024	7.1	Windows NTLM Spoofing Vulnerability **CVE ID: CVE-2024-30081**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30081	O-MIC-WIND-240724/4368
N/A	09-Jul-2024	6.5	Windows Line Printer Daemon Service Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38027	O-MIC-WIND-240724/4369

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38027		
Out-of-bounds Read	09-Jul-2024	6.5	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability **CVE ID: CVE-2024-38048**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38048	O-MIC-WIND-240724/4370
N/A	09-Jul-2024	5.9	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38099**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38099	O-MIC-WIND-240724/4371
N/A	09-Jul-2024	5.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID: CVE-2024-38017**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38017	O-MIC-WIND-240724/4372
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38055	O-MIC-WIND-240724/4373
N/A	09-Jul-2024	5.3	Windows iSCSI Service Denial of Service Vulnerability **CVE ID: CVE-2024-35270**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35270	O-MIC-WIND-240724/4374
Product: windows_server_2012					
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
N/A	09-Jul-2024	9.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38074**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38074	O-MIC-WIND-240724/4375
N/A	09-Jul-2024	9.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38077**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38077	O-MIC-WIND-240724/4376
N/A	09-Jul-2024	8.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-28899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28899	O-MIC-WIND-240724/4377
Out-of-bounds Write	09-Jul-2024	8.8	Windows Imaging Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38060**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38060	O-MIC-WIND-240724/4378
Use After Free	09-Jul-2024	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability **CVE ID: CVE-2024-38053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38053	O-MIC-WIND-240724/4379
Improper Restriction of Operations within the Bounds of a	09-Jul-2024	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38104**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38104	O-MIC-WIND-240724/4380

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Buffer					
N/A	09-Jul-2024	8.4	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37984	O-MIC-WIND-240724/4381
Externally Controlled Reference to a Resource in Another Sphere	09-Jul-2024	8.1	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability **CVE ID: CVE-2024-38049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38049	O-MIC-WIND-240724/4382
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37969**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37969	O-MIC-WIND-240724/4383
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37970**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37970	O-MIC-WIND-240724/4384
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37971**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37971	O-MIC-WIND-240724/4385
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4386

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-37972	lity/CVE-2024-37972	
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37989**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37989	O-MIC-WIND-240724/4387
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37974**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37974	O-MIC-WIND-240724/4388
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37975**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37975	O-MIC-WIND-240724/4389
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37986**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37986	O-MIC-WIND-240724/4390
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37987**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37987	O-MIC-WIND-240724/4391
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37988**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37988	O-MIC-WIND-240724/4392

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38010**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38010	O-MIC-WIND-240724/4393
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38011**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38011	O-MIC-WIND-240724/4394
Use After Free	09-Jul-2024	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38066**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38066	O-MIC-WIND-240724/4395
N/A	09-Jul-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37973**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37973	O-MIC-WIND-240724/4396
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38057	O-MIC-WIND-240724/4397
Out-of-bounds Write	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38054	O-MIC-WIND-240724/4398

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38052	O-MIC-WIND-240724/4399
Out-of-bounds Write	09-Jul-2024	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38051**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38051	O-MIC-WIND-240724/4400
Integer Underflow (Wrap or Wraparound)	09-Jul-2024	7.8	Windows Workstation Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38050**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38050	O-MIC-WIND-240724/4401
N/A	09-Jul-2024	7.8	Windows Filtering Platform Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38034	O-MIC-WIND-240724/4402
N/A	09-Jul-2024	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38079	O-MIC-WIND-240724/4403
N/A	09-Jul-2024	7.5	Windows TCP/IP Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4404

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38064	lity/CVE-2024-38064	
N/A	09-Jul-2024	7.5	DCOM Remote Cross-Session Activation Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38061	O-MIC-WIND-240724/4405
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38067**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38067	O-MIC-WIND-240724/4406
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38068**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38068	O-MIC-WIND-240724/4407
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38071**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38071	O-MIC-WIND-240724/4408
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38073**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38073	O-MIC-WIND-240724/4409

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	7.5	Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability **CVE ID: CVE-2024-38015**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38015	O-MIC-WIND-240724/4410
N/A	09-Jul-2024	7.5	Microsoft WS-Discovery Denial of Service Vulnerability **CVE ID: CVE-2024-38091**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38091	O-MIC-WIND-240724/4411
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38031**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38031	O-MIC-WIND-240724/4412
N/A	09-Jul-2024	7.3	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38033**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38033	O-MIC-WIND-240724/4413
Integer Overflow or Wraparound	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38019**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38019	O-MIC-WIND-240724/4414
Out-of-bounds Read	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4415

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID: CVE-2024-38028**	lity/CVE-2024-38028	
Out-of-bounds Write	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38025**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38025	O-MIC-WIND-240724/4416
Incorrect Conversion between Numeric Types	09-Jul-2024	7.2	DHCP Server Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38044**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38044	O-MIC-WIND-240724/4417
N/A	09-Jul-2024	7.1	Windows NTLM Spoofing Vulnerability **CVE ID: CVE-2024-30081**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30081	O-MIC-WIND-240724/4418
Improper Link Resolution Before File Access ('Link Following')	09-Jul-2024	7	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38022**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38022	O-MIC-WIND-240724/4419
N/A	09-Jul-2024	6.8	BitLocker Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38058**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38058	O-MIC-WIND-240724/4420
N/A	09-Jul-2024	6.7	Microsoft Windows Server Backup Elevation of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4421

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38013**	lity/CVE-2024-38013	
Out-of-bounds Read	09-Jul-2024	6.5	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability **CVE ID: CVE-2024-38048**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38048	O-MIC-WIND-240724/4422
N/A	09-Jul-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID: CVE-2024-38030**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38030	O-MIC-WIND-240724/4423
N/A	09-Jul-2024	6.5	Windows Line Printer Daemon Service Denial of Service Vulnerability **CVE ID: CVE-2024-38027**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38027	O-MIC-WIND-240724/4424
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38101**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38101	O-MIC-WIND-240724/4425
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38102**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38102	O-MIC-WIND-240724/4426

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38105**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38105	O-MIC-WIND-240724/4427
N/A	09-Jul-2024	5.9	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38099**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38099	O-MIC-WIND-240724/4428
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38056	O-MIC-WIND-240724/4429
N/A	09-Jul-2024	5.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID: CVE-2024-38017**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38017	O-MIC-WIND-240724/4430
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38055	O-MIC-WIND-240724/4431
N/A	09-Jul-2024	5.3	Windows iSCSI Service Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4432

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-35270	lity/CVE-2024-35270	
Affected Version(s): r2					
N/A	09-Jul-2024	9.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38077**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38077	O-MIC-WIND-240724/4433
N/A	09-Jul-2024	9.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38074**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38074	O-MIC-WIND-240724/4434
N/A	09-Jul-2024	8.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-28899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28899	O-MIC-WIND-240724/4435
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jul-2024	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38104**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38104	O-MIC-WIND-240724/4436
Out-of-bounds Write	09-Jul-2024	8.8	Windows Imaging Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38060**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38060	O-MIC-WIND-240724/4437
Use After Free	09-Jul-2024	8.8	Windows Layer-2 Bridge Network	https://msrc.microsoft.com/up	O-MIC-WIND-240724/4438

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Driver Remote Code Execution Vulnerability **CVE ID: CVE-2024-38053**	date-guide/vulnerability/CVE-2024-38053	
N/A	09-Jul-2024	8.4	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37984	O-MIC-WIND-240724/4439
Externally Controlled Reference to a Resource in Another Sphere	09-Jul-2024	8.1	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability **CVE ID: CVE-2024-38049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38049	O-MIC-WIND-240724/4440
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37969**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37969	O-MIC-WIND-240724/4441
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37970**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37970	O-MIC-WIND-240724/4442
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37971**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37971	O-MIC-WIND-240724/4443
N/A	09-Jul-2024	8	Secure Boot Security Feature	https://msrc.microsoft.com/up	O-MIC-WIND-240724/4444

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
			Bypass Vulnerability **CVE ID: CVE-2024-37972**	date-guide/vulnerability/CVE-2024-37972	
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37974**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37974	O-MIC-WIND-240724/4445
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37975**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37975	O-MIC-WIND-240724/4446
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37986**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37986	O-MIC-WIND-240724/4447
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37987**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37987	O-MIC-WIND-240724/4448
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37988**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37988	O-MIC-WIND-240724/4449
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37989	O-MIC-WIND-240724/4450

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-37989		
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38010**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38010	O-MIC-WIND-240724/4451
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38011**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38011	O-MIC-WIND-240724/4452
N/A	09-Jul-2024	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38079	O-MIC-WIND-240724/4453
N/A	09-Jul-2024	7.8	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability **CVE ID: CVE-2024-30079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30079	O-MIC-WIND-240724/4454
N/A	09-Jul-2024	7.8	Windows Filtering Platform Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38034	O-MIC-WIND-240724/4455
Integer Underflow (Wrap or Wraparound)	09-Jul-2024	7.8	Windows Workstation Service Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38050	O-MIC-WIND-240724/4456

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38050		
Out-of-bounds Write	09-Jul-2024	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38051**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38051	O-MIC-WIND-240724/4457
N/A	09-Jul-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37973**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37973	O-MIC-WIND-240724/4458
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38052	O-MIC-WIND-240724/4459
Out-of-bounds Write	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38054	O-MIC-WIND-240724/4460
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38057	O-MIC-WIND-240724/4461

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38066**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38066	O-MIC-WIND-240724/4462
N/A	09-Jul-2024	7.5	Windows TCP/IP Information Disclosure Vulnerability **CVE ID: CVE-2024-38064**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38064	O-MIC-WIND-240724/4463
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38071**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38071	O-MIC-WIND-240724/4464
N/A	09-Jul-2024	7.5	Windows Cryptographic Services Security Feature Bypass Vulnerability **CVE ID: CVE-2024-30098**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30098	O-MIC-WIND-240724/4465
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38073**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38073	O-MIC-WIND-240724/4466
N/A	09-Jul-2024	7.5	Microsoft WS-Discovery Denial of Service Vulnerability **CVE ID: CVE-2024-38091**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38091	O-MIC-WIND-240724/4467

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	7.5	Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability **CVE ID: CVE-2024-38015**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38015	O-MIC-WIND-240724/4468
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38031**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38031	O-MIC-WIND-240724/4469
N/A	09-Jul-2024	7.5	DCOM Remote Cross-Session Activation Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38061	O-MIC-WIND-240724/4470
User Interface (UI) Misrepresentation of Critical Information	09-Jul-2024	7.5	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-38112**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112	O-MIC-WIND-240724/4471
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38067**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38067	O-MIC-WIND-240724/4472
N/A	09-Jul-2024	7.5	Windows Online Certificate Status	https://msrc.microsoft.com/up	O-MIC-WIND-240724/4473

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38068**	date-guide/vulnerability/CVE-2024-38068	
N/A	09-Jul-2024	7.3	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38033**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38033	O-MIC-WIND-240724/4474
Integer Overflow or Wraparound	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38019**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38019	O-MIC-WIND-240724/4475
Out-of-bounds Write	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38025**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38025	O-MIC-WIND-240724/4476
Incorrect Conversion between Numeric Types	09-Jul-2024	7.2	DHCP Server Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38044**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38044	O-MIC-WIND-240724/4477
Out-of-bounds Read	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38028	O-MIC-WIND-240724/4478

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38028		
N/A	09-Jul-2024	7.1	Windows NTLM Spoofing Vulnerability **CVE ID: CVE-2024-30081**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30081	O-MIC-WIND-240724/4479
Improper Link Resolution Before File Access ('Link Following')	09-Jul-2024	7	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38022**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38022	O-MIC-WIND-240724/4480
N/A	09-Jul-2024	6.8	BitLocker Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38058**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38058	O-MIC-WIND-240724/4481
Out-of-bounds Write	09-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38065**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38065	O-MIC-WIND-240724/4482
N/A	09-Jul-2024	6.7	Microsoft Windows Server Backup Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38013	O-MIC-WIND-240724/4483
Out-of-bounds Read	09-Jul-2024	6.5	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38048	O-MIC-WIND-240724/4484

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38048		
N/A	09-Jul-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID: CVE-2024-38030**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38030	O-MIC-WIND-240724/4485
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38101**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38101	O-MIC-WIND-240724/4486
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38102**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38102	O-MIC-WIND-240724/4487
N/A	09-Jul-2024	6.5	Windows Line Printer Daemon Service Denial of Service Vulnerability **CVE ID: CVE-2024-38027**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38027	O-MIC-WIND-240724/4488
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38105**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38105	O-MIC-WIND-240724/4489
N/A	09-Jul-2024	5.9	Windows Remote Desktop Licensing Service Denial of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4490

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Vulnerability **CVE ID: CVE-2024-38099**	lity/CVE-2024-38099	
N/A	09-Jul-2024	5.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID: CVE-2024-38017**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38017	O-MIC-WIND-240724/4491
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38055	O-MIC-WIND-240724/4492
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38056	O-MIC-WIND-240724/4493
N/A	09-Jul-2024	5.3	Windows iSCSI Service Denial of Service Vulnerability **CVE ID: CVE-2024-35270**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35270	O-MIC-WIND-240724/4494
N/A	09-Jul-2024	4.7	Windows Remote Access Connection Manager Information Disclosure Vulnerability **CVE ID: CVE-2024-30071**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30071	O-MIC-WIND-240724/4495
Product: windows_server_2016					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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) 10.0.14393.7159					
N/A	09-Jul-2024	9.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38076**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38076	O-MIC-WIND-240724/4496
N/A	09-Jul-2024	9.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38077**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38077	O-MIC-WIND-240724/4497
N/A	09-Jul-2024	9.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38074**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38074	O-MIC-WIND-240724/4498
N/A	09-Jul-2024	8.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-28899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28899	O-MIC-WIND-240724/4499
N/A	09-Jul-2024	8.8	Windows MultiPoint Services Remote Code Execution Vulnerability **CVE ID: CVE-2024-30013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30013	O-MIC-WIND-240724/4500
Use After Free	09-Jul-2024	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4501

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38053	lity/CVE-2024-38053	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jul-2024	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38104**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38104	O-MIC-WIND-240724/4502
Out-of-bounds Write	09-Jul-2024	8.8	Windows Imaging Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38060**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38060	O-MIC-WIND-240724/4503
N/A	09-Jul-2024	8.4	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37984	O-MIC-WIND-240724/4504
Externally Controlled Reference to a Resource in Another Sphere	09-Jul-2024	8.1	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability **CVE ID: CVE-2024-38049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38049	O-MIC-WIND-240724/4505
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37969**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37969	O-MIC-WIND-240724/4506
N/A	09-Jul-2024	8	Secure Boot Security Feature	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/4507

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bypass Vulnerability **CVE ID: CVE-2024-37970**	guide/vulnerability/CVE-2024-37970	
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37971**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37971	O-MIC-WIND-240724/4508
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37972**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37972	O-MIC-WIND-240724/4509
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37974**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37974	O-MIC-WIND-240724/4510
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37975**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37975	O-MIC-WIND-240724/4511
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37986**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37986	O-MIC-WIND-240724/4512
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37987	O-MIC-WIND-240724/4513

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-37987		
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38010**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38010	O-MIC-WIND-240724/4514
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38011**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38011	O-MIC-WIND-240724/4515
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37988**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37988	O-MIC-WIND-240724/4516
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37989**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37989	O-MIC-WIND-240724/4517
N/A	09-Jul-2024	7.8	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability **CVE ID: CVE-2024-30079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30079	O-MIC-WIND-240724/4518
N/A	09-Jul-2024	7.8	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38070**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38070	O-MIC-WIND-240724/4519

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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)	09-Jul-2024	7.8	Windows Workstation Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38050**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38050	O-MIC-WIND-240724/4520
N/A	09-Jul-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37973**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37973	O-MIC-WIND-240724/4521
Use After Free	09-Jul-2024	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38066**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38066	O-MIC-WIND-240724/4522
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38043	O-MIC-WIND-240724/4523
N/A	09-Jul-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38062	O-MIC-WIND-240724/4524
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38057	O-MIC-WIND-240724/4525

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38054	O-MIC-WIND-240724/4526
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38047**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38047	O-MIC-WIND-240724/4527
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38052	O-MIC-WIND-240724/4528
Out-of-bounds Write	09-Jul-2024	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38051**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38051	O-MIC-WIND-240724/4529
N/A	09-Jul-2024	7.8	Windows Filtering Platform Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38034	O-MIC-WIND-240724/4530
N/A	09-Jul-2024	7.8	Windows Graphics Component Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4531

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38079	lity/CVE-2024-38079	
N/A	09-Jul-2024	7.8	Windows File Explorer Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38100**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38100	O-MIC-WIND-240724/4532
N/A	09-Jul-2024	7.5	DCOM Remote Cross-Session Activation Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38061	O-MIC-WIND-240724/4533
N/A	09-Jul-2024	7.5	Windows TCP/IP Information Disclosure Vulnerability **CVE ID: CVE-2024-38064**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38064	O-MIC-WIND-240724/4534
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38068**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38068	O-MIC-WIND-240724/4535
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38071**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38071	O-MIC-WIND-240724/4536
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/4537

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Vulnerability **CVE ID: CVE-2024-38072**	guide/vulnerability/CVE-2024-38072	
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38073**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38073	O-MIC-WIND-240724/4538
N/A	09-Jul-2024	7.5	Windows Cryptographic Services Security Feature Bypass Vulnerability **CVE ID: CVE-2024-30098**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30098	O-MIC-WIND-240724/4539
N/A	09-Jul-2024	7.5	Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability **CVE ID: CVE-2024-38015**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38015	O-MIC-WIND-240724/4540
N/A	09-Jul-2024	7.5	Microsoft WS-Discovery Denial of Service Vulnerability **CVE ID: CVE-2024-38091**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38091	O-MIC-WIND-240724/4541
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38031**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38031	O-MIC-WIND-240724/4542

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38067**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38067	O-MIC-WIND-240724/4543
User Interface (UI) Misrepresentation of Critical Information	09-Jul-2024	7.5	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-38112**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112	O-MIC-WIND-240724/4544
N/A	09-Jul-2024	7.3	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38033**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38033	O-MIC-WIND-240724/4545
Incorrect Conversion between Numeric Types	09-Jul-2024	7.2	DHCP Server Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38044**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38044	O-MIC-WIND-240724/4546
Out-of-bounds Read	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38028**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38028	O-MIC-WIND-240724/4547
Out-of-bounds Write	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4548

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID: CVE-2024-38025**	lity/CVE-2024-38025	
Integer Overflow or Wraparound	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38019**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38019	O-MIC-WIND-240724/4549
N/A	09-Jul-2024	7.1	Windows NTLM Spoofing Vulnerability **CVE ID: CVE-2024-30081**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30081	O-MIC-WIND-240724/4550
Improper Verification of Cryptographic Signature	09-Jul-2024	7	Windows Enroll Engine Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38069**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38069	O-MIC-WIND-240724/4551
Improper Link Resolution Before File Access ('Link Following')	09-Jul-2024	7	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38022**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38022	O-MIC-WIND-240724/4552
Out-of-bounds Write	09-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38065**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38065	O-MIC-WIND-240724/4553
N/A	09-Jul-2024	6.8	BitLocker Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/4554

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38058	guide/vulnerability/CVE-2024-38058	
N/A	09-Jul-2024	6.7	Microsoft Windows Server Backup Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38013	O-MIC-WIND-240724/4555
Out-of-bounds Read	09-Jul-2024	6.5	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability **CVE ID: CVE-2024-38048**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38048	O-MIC-WIND-240724/4556
N/A	09-Jul-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID: CVE-2024-38030**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38030	O-MIC-WIND-240724/4557
N/A	09-Jul-2024	6.5	Windows Line Printer Daemon Service Denial of Service Vulnerability **CVE ID: CVE-2024-38027**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38027	O-MIC-WIND-240724/4558
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38101**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38101	O-MIC-WIND-240724/4559
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/4560

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Vulnerability **CVE ID: CVE-2024-38102**	guide/vulnerability/CVE-2024-38102	
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38105**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38105	O-MIC-WIND-240724/4561
N/A	09-Jul-2024	5.9	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38099**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38099	O-MIC-WIND-240724/4562
N/A	09-Jul-2024	5.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID: CVE-2024-38017**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38017	O-MIC-WIND-240724/4563
N/A	09-Jul-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38041**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38041	O-MIC-WIND-240724/4564
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38055	O-MIC-WIND-240724/4565
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library	https://msrc.microsoft.com/up	O-MIC-WIND-240724/4566

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38056**	date-guide/vulnerability/CVE-2024-38056	
N/A	09-Jul-2024	5.3	Windows iSCSI Service Denial of Service Vulnerability **CVE ID: CVE-2024-35270**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35270	O-MIC-WIND-240724/4567
N/A	09-Jul-2024	4.7	Windows Remote Access Connection Manager Information Disclosure Vulnerability **CVE ID: CVE-2024-30071**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30071	O-MIC-WIND-240724/4568
Product: windows_server_2019					
Affected Version(s): * Up to (excluding) 10.0.17763.6054					
N/A	09-Jul-2024	9.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38076**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38076	O-MIC-WIND-240724/4569
N/A	09-Jul-2024	9.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38077**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38077	O-MIC-WIND-240724/4570
N/A	09-Jul-2024	9.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4571

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-2024-38074	lity/CVE-2024-38074	
N/A	09-Jul-2024	8.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-28899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28899	O-MIC-WIND-240724/4572
N/A	09-Jul-2024	8.8	Windows MultiPoint Services Remote Code Execution Vulnerability **CVE ID: CVE-2024-30013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30013	O-MIC-WIND-240724/4573
Out-of-bounds Write	09-Jul-2024	8.8	Windows Imaging Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38060**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38060	O-MIC-WIND-240724/4574
Use After Free	09-Jul-2024	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability **CVE ID: CVE-2024-38053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38053	O-MIC-WIND-240724/4575
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jul-2024	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38104**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38104	O-MIC-WIND-240724/4576
N/A	09-Jul-2024	8.4	Secure Boot Security Feature	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4577

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bypass Vulnerability **CVE ID: CVE-2024-37984**	lity/CVE-2024-37984	
Externally Controlled Reference to a Resource in Another Sphere	09-Jul-2024	8.1	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability **CVE ID: CVE-2024-38049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38049	O-MIC-WIND-240724/4578
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37969**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37969	O-MIC-WIND-240724/4579
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37970**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37970	O-MIC-WIND-240724/4580
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37971**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37971	O-MIC-WIND-240724/4581
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37972**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37972	O-MIC-WIND-240724/4582
N/A	09-Jul-2024	8	Secure Boot Security Feature	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/4583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bypass Vulnerability **CVE ID: CVE-2024-37974**	guide/vulnerability/CVE-2024-37974	
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37975**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37975	O-MIC-WIND-240724/4584
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37981**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37981	O-MIC-WIND-240724/4585
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37986**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37986	O-MIC-WIND-240724/4586
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37987**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37987	O-MIC-WIND-240724/4587
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38010**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38010	O-MIC-WIND-240724/4588
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38011	O-MIC-WIND-240724/4589

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38011		
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37988**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37988	O-MIC-WIND-240724/4590
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37989**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37989	O-MIC-WIND-240724/4591
N/A	09-Jul-2024	7.8	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability **CVE ID: CVE-2024-30079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30079	O-MIC-WIND-240724/4592
N/A	09-Jul-2024	7.8	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38070**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38070	O-MIC-WIND-240724/4593
Integer Underflow (Wrap or Wraparound)	09-Jul-2024	7.8	Windows Workstation Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38050**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38050	O-MIC-WIND-240724/4594
N/A	09-Jul-2024	7.8	Secure Boot Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4595

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
			CVE ID: CVE-2024-37973	lity/CVE-2024-37973	
Use After Free	09-Jul-2024	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38066**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38066	O-MIC-WIND-240724/4596
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38043	O-MIC-WIND-240724/4597
N/A	09-Jul-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38062	O-MIC-WIND-240724/4598
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38057	O-MIC-WIND-240724/4599
Out-of-bounds Write	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38054	O-MIC-WIND-240724/4600
N/A	09-Jul-2024	7.8	PowerShell Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/4601

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38047**	guide/vulnerability/CVE-2024-38047	
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38052	O-MIC-WIND-240724/4602
Out-of-bounds Write	09-Jul-2024	7.8	Windows Graphics Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38051**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38051	O-MIC-WIND-240724/4603
N/A	09-Jul-2024	7.8	Windows Filtering Platform Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38034	O-MIC-WIND-240724/4604
N/A	09-Jul-2024	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38079	O-MIC-WIND-240724/4605
N/A	09-Jul-2024	7.8	Windows File Explorer Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38100**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38100	O-MIC-WIND-240724/4606
N/A	09-Jul-2024	7.5	DCOM Remote Cross-Session	https://msrc.microsoft.com/up	O-MIC-WIND-240724/4607

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Activation Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38061**	date-guide/vulnerability/CVE-2024-38061	
N/A	09-Jul-2024	7.5	Windows TCP/IP Information Disclosure Vulnerability **CVE ID: CVE-2024-38064**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38064	O-MIC-WIND-240724/4608
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38068**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38068	O-MIC-WIND-240724/4609
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38071**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38071	O-MIC-WIND-240724/4610
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38072**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38072	O-MIC-WIND-240724/4611
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38073	O-MIC-WIND-240724/4612

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38073		
N/A	09-Jul-2024	7.5	Windows Cryptographic Services Security Feature Bypass Vulnerability **CVE ID: CVE-2024-30098**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30098	O-MIC-WIND-240724/4613
N/A	09-Jul-2024	7.5	Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability **CVE ID: CVE-2024-38015**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38015	O-MIC-WIND-240724/4614
N/A	09-Jul-2024	7.5	Microsoft WS-Discovery Denial of Service Vulnerability **CVE ID: CVE-2024-38091**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38091	O-MIC-WIND-240724/4615
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38031**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38031	O-MIC-WIND-240724/4616
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38067**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38067	O-MIC-WIND-240724/4617

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Interface (UI) Misrepresentation of Critical Information	09-Jul-2024	7.5	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-38112**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112	O-MIC-WIND-240724/4618
N/A	09-Jul-2024	7.3	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38033**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38033	O-MIC-WIND-240724/4619
Incorrect Conversion between Numeric Types	09-Jul-2024	7.2	DHCP Server Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38044**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38044	O-MIC-WIND-240724/4620
Out-of-bounds Read	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38028**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38028	O-MIC-WIND-240724/4621
Out-of-bounds Write	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38025**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38025	O-MIC-WIND-240724/4622
Integer Overflow or Wraparound	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4623

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
			Execution Vulnerability **CVE ID: CVE-2024-38019**	lity/CVE-2024-38019	
N/A	09-Jul-2024	7.1	Windows NTLM Spoofing Vulnerability **CVE ID: CVE-2024-30081**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30081	O-MIC-WIND-240724/4624
Improper Verification of Cryptographic Signature	09-Jul-2024	7	Windows Enroll Engine Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38069**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38069	O-MIC-WIND-240724/4625
Improper Link Resolution Before File Access ('Link Following')	09-Jul-2024	7	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38022**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38022	O-MIC-WIND-240724/4626
Out-of-bounds Write	09-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38065**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38065	O-MIC-WIND-240724/4627
N/A	09-Jul-2024	6.8	BitLocker Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38058**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38058	O-MIC-WIND-240724/4628
N/A	09-Jul-2024	6.7	Microsoft Windows Server Backup Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4629

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38013	lity/CVE-2024-38013	
Out-of-bounds Read	09-Jul-2024	6.5	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability **CVE ID: CVE-2024-38048**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38048	O-MIC-WIND-240724/4630
N/A	09-Jul-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID: CVE-2024-38030**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38030	O-MIC-WIND-240724/4631
N/A	09-Jul-2024	6.5	Windows Line Printer Daemon Service Denial of Service Vulnerability **CVE ID: CVE-2024-38027**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38027	O-MIC-WIND-240724/4632
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38101**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38101	O-MIC-WIND-240724/4633
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38102**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38102	O-MIC-WIND-240724/4634
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4635

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Vulnerability **CVE ID: CVE-2024-38105**	lity/CVE-2024-38105	
N/A	09-Jul-2024	5.9	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38099**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38099	O-MIC-WIND-240724/4636
N/A	09-Jul-2024	5.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID: CVE-2024-38017**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38017	O-MIC-WIND-240724/4637
N/A	09-Jul-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38041**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38041	O-MIC-WIND-240724/4638
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38055	O-MIC-WIND-240724/4639
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38056	O-MIC-WIND-240724/4640
N/A	09-Jul-2024	5.3	Windows iSCSI Service Denial of	https://msrc.microsoft.com/up	O-MIC-WIND-240724/4641

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Vulnerability **CVE ID: CVE-2024-35270**	date-guide/vulnerability/CVE-2024-35270	
N/A	09-Jul-2024	4.7	Windows Remote Access Connection Manager Information Disclosure Vulnerability **CVE ID: CVE-2024-30071**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30071	O-MIC-WIND-240724/4642
Product: windows_server_2022					
Affected Version(s): * Up to (excluding) 10.0.20348.2582					
N/A	09-Jul-2024	9.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38077**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38077	O-MIC-WIND-240724/4643
N/A	09-Jul-2024	9.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38074**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38074	O-MIC-WIND-240724/4644
N/A	09-Jul-2024	9.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38076**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38076	O-MIC-WIND-240724/4645
Improper Restriction of Operations within the	09-Jul-2024	8.8	Windows Fax Service Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4646

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
Bounds of a Memory Buffer			**CVE ID: CVE-2024-38104**	lity/CVE-2024-38104	
N/A	09-Jul-2024	8.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-28899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28899	O-MIC-WIND-240724/4647
N/A	09-Jul-2024	8.8	Windows MultiPoint Services Remote Code Execution Vulnerability **CVE ID: CVE-2024-30013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30013	O-MIC-WIND-240724/4648
Out-of-bounds Write	09-Jul-2024	8.8	Windows Imaging Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38060**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38060	O-MIC-WIND-240724/4649
Use After Free	09-Jul-2024	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability **CVE ID: CVE-2024-38053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38053	O-MIC-WIND-240724/4650
N/A	09-Jul-2024	8.4	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37984	O-MIC-WIND-240724/4651
Externally Controlled Reference to a	09-Jul-2024	8.1	Windows Distributed Transaction Coordinator	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource in Another Sphere			Remote Code Execution Vulnerability **CVE ID: CVE-2024-38049**	lity/CVE-2024-38049	
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37969**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37969	O-MIC-WIND-240724/4653
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37970**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37970	O-MIC-WIND-240724/4654
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37987**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37987	O-MIC-WIND-240724/4655
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37972**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37972	O-MIC-WIND-240724/4656
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37974**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37974	O-MIC-WIND-240724/4657
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4658

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-37975	lity/CVE-2024-37975	
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37977**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37977	O-MIC-WIND-240724/4659
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37981**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37981	O-MIC-WIND-240724/4660
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37986**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37986	O-MIC-WIND-240724/4661
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37988**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37988	O-MIC-WIND-240724/4662
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37971**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37971	O-MIC-WIND-240724/4663
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38010**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38010	O-MIC-WIND-240724/4664

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38011**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38011	O-MIC-WIND-240724/4665
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37989**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37989	O-MIC-WIND-240724/4666
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38043	O-MIC-WIND-240724/4667
N/A	09-Jul-2024	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38079	O-MIC-WIND-240724/4668
N/A	09-Jul-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38059**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38059	O-MIC-WIND-240724/4669
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38057	O-MIC-WIND-240724/4670

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38054	O-MIC-WIND-240724/4671
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38047**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38047	O-MIC-WIND-240724/4672
N/A	09-Jul-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37973**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37973	O-MIC-WIND-240724/4673
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38052	O-MIC-WIND-240724/4674
N/A	09-Jul-2024	7.8	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38070**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38070	O-MIC-WIND-240724/4675
Out-of-bounds Write	09-Jul-2024	7.8	Windows Graphics Component Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4676

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38051	lity/CVE-2024-38051	
N/A	09-Jul-2024	7.8	Windows Filtering Platform Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38034	O-MIC-WIND-240724/4677
Integer Underflow (Wrap or Wraparound)	09-Jul-2024	7.8	Windows Workstation Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38050**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38050	O-MIC-WIND-240724/4678
N/A	09-Jul-2024	7.8	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability **CVE ID: CVE-2024-30079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30079	O-MIC-WIND-240724/4679
N/A	09-Jul-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38080**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38080	O-MIC-WIND-240724/4680
N/A	09-Jul-2024	7.8	Windows File Explorer Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38100**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38100	O-MIC-WIND-240724/4681
N/A	09-Jul-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38062	O-MIC-WIND-240724/4682

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38062		
N/A	09-Jul-2024	7.5	Windows TCP/IP Information Disclosure Vulnerability **CVE ID: CVE-2024-38064**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38064	O-MIC-WIND-240724/4683
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38067**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38067	O-MIC-WIND-240724/4684
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38071**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38071	O-MIC-WIND-240724/4685
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38072**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38072	O-MIC-WIND-240724/4686
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38073**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38073	O-MIC-WIND-240724/4687
N/A	09-Jul-2024	7.5	Windows Cryptographic Services Security	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/4688

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Feature Bypass Vulnerability **CVE ID: CVE-2024-30098**	guide/vulnerability/CVE-2024-30098	
N/A	09-Jul-2024	7.5	Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability **CVE ID: CVE-2024-38015**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38015	O-MIC-WIND-240724/4689
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38031**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38031	O-MIC-WIND-240724/4690
N/A	09-Jul-2024	7.5	Microsoft WS-Discovery Denial of Service Vulnerability **CVE ID: CVE-2024-38091**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38091	O-MIC-WIND-240724/4691
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38068**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38068	O-MIC-WIND-240724/4692
N/A	09-Jul-2024	7.5	DCOM Remote Cross-Session Activation Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38061	O-MIC-WIND-240724/4693

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38061		
User Interface (UI) Misrepresentation of Critical Information	09-Jul-2024	7.5	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-38112**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112	O-MIC-WIND-240724/4694
N/A	09-Jul-2024	7.3	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38033**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38033	O-MIC-WIND-240724/4695
Incorrect Conversion between Numeric Types	09-Jul-2024	7.2	DHCP Server Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38044**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38044	O-MIC-WIND-240724/4696
Out-of-bounds Read	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38028**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38028	O-MIC-WIND-240724/4697
Out-of-bounds Write	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38025**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38025	O-MIC-WIND-240724/4698
Integer Overflow or	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/4699

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Remote Code Execution Vulnerability **CVE ID: CVE-2024-38019**	guide/vulnerability/CVE-2024-38019	
N/A	09-Jul-2024	7.1	Windows NTLM Spoofing Vulnerability **CVE ID: CVE-2024-30081**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30081	O-MIC-WIND-240724/4700
Improper Verification of Cryptographic Signature	09-Jul-2024	7	Windows Enroll Engine Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38069**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38069	O-MIC-WIND-240724/4701
Improper Link Resolution Before File Access ('Link Following')	09-Jul-2024	7	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38022**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38022	O-MIC-WIND-240724/4702
Out-of-bounds Write	09-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38065**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38065	O-MIC-WIND-240724/4703
N/A	09-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-26184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26184	O-MIC-WIND-240724/4704
N/A	09-Jul-2024	6.8	BitLocker Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4705

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38058	lity/CVE-2024-38058	
N/A	09-Jul-2024	6.7	Microsoft Windows Server Backup Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38013	O-MIC-WIND-240724/4706
Out-of-bounds Read	09-Jul-2024	6.5	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability **CVE ID: CVE-2024-38048**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38048	O-MIC-WIND-240724/4707
N/A	09-Jul-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID: CVE-2024-38030**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38030	O-MIC-WIND-240724/4708
N/A	09-Jul-2024	6.5	Windows Line Printer Daemon Service Denial of Service Vulnerability **CVE ID: CVE-2024-38027**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38027	O-MIC-WIND-240724/4709
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38101**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38101	O-MIC-WIND-240724/4710
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4711

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Vulnerability **CVE ID: CVE-2024-38102**	lity/CVE-2024-38102	
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38105**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38105	O-MIC-WIND-240724/4712
N/A	09-Jul-2024	5.9	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38099**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38099	O-MIC-WIND-240724/4713
N/A	09-Jul-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38041**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38041	O-MIC-WIND-240724/4714
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38055	O-MIC-WIND-240724/4715
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38056	O-MIC-WIND-240724/4716
N/A	09-Jul-2024	5.5	Microsoft Message Queuing	https://msrc.microsoft.com/up	O-MIC-WIND-240724/4717

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38017**	date-guide/vulnerability/CVE-2024-38017	
N/A	09-Jul-2024	5.3	Windows iSCSI Service Denial of Service Vulnerability **CVE ID: CVE-2024-35270**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35270	O-MIC-WIND-240724/4718
Product: windows_server_2022_23h2					
Affected Version(s): * Up to (excluding) 10.0.25398.1009					
N/A	09-Jul-2024	9.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38076**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38076	O-MIC-WIND-240724/4719
N/A	09-Jul-2024	9.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38074**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38074	O-MIC-WIND-240724/4720
N/A	09-Jul-2024	9.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38077**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38077	O-MIC-WIND-240724/4721
Improper Restriction of Operations within the Bounds of a	09-Jul-2024	8.8	Windows Fax Service Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38104	O-MIC-WIND-240724/4722

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Buffer			**CVE ID: CVE-2024-38104**		
N/A	09-Jul-2024	8.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-28899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28899	O-MIC-WIND-240724/4723
N/A	09-Jul-2024	8.8	Windows MultiPoint Services Remote Code Execution Vulnerability **CVE ID: CVE-2024-30013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30013	O-MIC-WIND-240724/4724
Use After Free	09-Jul-2024	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability **CVE ID: CVE-2024-38053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38053	O-MIC-WIND-240724/4725
Out-of-bounds Write	09-Jul-2024	8.8	Windows Imaging Component Remote Code Execution Vulnerability **CVE ID: CVE-2024-38060**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38060	O-MIC-WIND-240724/4726
N/A	09-Jul-2024	8.4	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37984	O-MIC-WIND-240724/4727
Externally Controlled Reference to a Resource	09-Jul-2024	8.1	Windows Distributed Transaction Coordinator Remote Code	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4728

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Another Sphere			Execution Vulnerability **CVE ID: CVE-2024-38049**	lity/CVE-2024-38049	
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37969**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37969	O-MIC-WIND-240724/4729
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37970**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37970	O-MIC-WIND-240724/4730
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37971**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37971	O-MIC-WIND-240724/4731
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37972**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37972	O-MIC-WIND-240724/4732
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37974**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37974	O-MIC-WIND-240724/4733
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37975	O-MIC-WIND-240724/4734

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
			CVE ID: CVE-2024-37975		
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37977**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37977	O-MIC-WIND-240724/4735
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38010**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38010	O-MIC-WIND-240724/4736
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38011**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38011	O-MIC-WIND-240724/4737
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37981**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37981	O-MIC-WIND-240724/4738
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37978**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37978	O-MIC-WIND-240724/4739
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37986**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37986	O-MIC-WIND-240724/4740

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	7.8	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability **CVE ID: CVE-2024-30079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30079	O-MIC-WIND-240724/4741
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38043	O-MIC-WIND-240724/4742
N/A	09-Jul-2024	7.8	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38070**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38070	O-MIC-WIND-240724/4743
N/A	09-Jul-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37973**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37973	O-MIC-WIND-240724/4744
N/A	09-Jul-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38062	O-MIC-WIND-240724/4745
N/A	09-Jul-2024	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38079**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38079	O-MIC-WIND-240724/4746

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	09-Jul-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38059**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38059	O-MIC-WIND-240724/4747
Out-of-bounds Write	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38054	O-MIC-WIND-240724/4748
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38057	O-MIC-WIND-240724/4749
N/A	09-Jul-2024	7.8	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38052	O-MIC-WIND-240724/4750
N/A	09-Jul-2024	7.8	PowerShell Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38047**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38047	O-MIC-WIND-240724/4751
Out-of-bounds Write	09-Jul-2024	7.8	Windows Graphics Component Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4752

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38051	lity/CVE-2024-38051	
N/A	09-Jul-2024	7.8	Windows Filtering Platform Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38034	O-MIC-WIND-240724/4753
Integer Underflow (Wrap or Wraparound)	09-Jul-2024	7.8	Windows Workstation Service Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38050**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38050	O-MIC-WIND-240724/4754
N/A	09-Jul-2024	7.8	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38080**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38080	O-MIC-WIND-240724/4755
N/A	09-Jul-2024	7.8	Windows File Explorer Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38100**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38100	O-MIC-WIND-240724/4756
N/A	09-Jul-2024	7.5	DCOM Remote Cross-Session Activation Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38061	O-MIC-WIND-240724/4757
N/A	09-Jul-2024	7.5	Windows TCP/IP Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4758

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38064	lity/CVE-2024-38064	
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38067**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38067	O-MIC-WIND-240724/4759
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38071**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38071	O-MIC-WIND-240724/4760
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38072**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38072	O-MIC-WIND-240724/4761
N/A	09-Jul-2024	7.5	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38073**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38073	O-MIC-WIND-240724/4762
N/A	09-Jul-2024	7.5	Windows Cryptographic Services Security Feature Bypass Vulnerability **CVE ID: CVE-2024-30098**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30098	O-MIC-WIND-240724/4763
N/A	09-Jul-2024	7.5	Windows Remote Desktop Gateway	https://msrc.microsoft.com/up	O-MIC-WIND-240724/4764

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(RD Gateway) Denial of Service Vulnerability **CVE ID: CVE-2024-38015**	date-guide/vulnerability/CVE-2024-38015	
N/A	09-Jul-2024	7.5	Microsoft WS-Discovery Denial of Service Vulnerability **CVE ID: CVE-2024-38091**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38091	O-MIC-WIND-240724/4765
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38031**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38031	O-MIC-WIND-240724/4766
N/A	09-Jul-2024	7.5	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability **CVE ID: CVE-2024-38068**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38068	O-MIC-WIND-240724/4767
User Interface (UI) Misrepresentation of Critical Information	09-Jul-2024	7.5	Windows MSHTML Platform Spoofing Vulnerability **CVE ID: CVE-2024-38112**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112	O-MIC-WIND-240724/4768
N/A	09-Jul-2024	7.3	PowerShell Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38033	O-MIC-WIND-240724/4769

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38033		
Incorrect Conversion between Numeric Types	09-Jul-2024	7.2	DHCP Server Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38044**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38044	O-MIC-WIND-240724/4770
Out-of-bounds Read	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38028**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38028	O-MIC-WIND-240724/4771
Out-of-bounds Write	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38025**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38025	O-MIC-WIND-240724/4772
Integer Overflow or Wraparound	09-Jul-2024	7.2	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability **CVE ID: CVE-2024-38019**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38019	O-MIC-WIND-240724/4773
N/A	09-Jul-2024	7.1	Windows NTLM Spoofing Vulnerability **CVE ID: CVE-2024-30081**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30081	O-MIC-WIND-240724/4774
Improper Verification of	09-Jul-2024	7	Windows Enroll Engine Security	https://msrc.microsoft.com/update-	O-MIC-WIND-240724/4775

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Signature			Feature Bypass Vulnerability **CVE ID: CVE-2024-38069**	guide/vulnerability/CVE-2024-38069	
Improper Link Resolution Before File Access ('Link Following')	09-Jul-2024	7	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38022**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38022	O-MIC-WIND-240724/4776
Out-of-bounds Write	09-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38065**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38065	O-MIC-WIND-240724/4777
N/A	09-Jul-2024	6.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-26184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26184	O-MIC-WIND-240724/4778
N/A	09-Jul-2024	6.8	BitLocker Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38058**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38058	O-MIC-WIND-240724/4779
N/A	09-Jul-2024	6.7	Microsoft Windows Server Backup Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38013**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38013	O-MIC-WIND-240724/4780
N/A	09-Jul-2024	6.5	Windows Line Printer Daemon Service Denial of	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-240724/4781

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
			Service Vulnerability **CVE ID: CVE-2024-38027**	lity/CVE-2024-38027	
Out-of-bounds Read	09-Jul-2024	6.5	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability **CVE ID: CVE-2024-38048**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38048	O-MIC-WIND-240724/4782
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38101**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38101	O-MIC-WIND-240724/4783
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38102**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38102	O-MIC-WIND-240724/4784
N/A	09-Jul-2024	6.5	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability **CVE ID: CVE-2024-38105**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38105	O-MIC-WIND-240724/4785
N/A	09-Jul-2024	5.9	Windows Remote Desktop Licensing Service Denial of Service Vulnerability **CVE ID: CVE-2024-38099**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38099	O-MIC-WIND-240724/4786

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
N/A	09-Jul-2024	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID: CVE-2024-38041**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38041	O-MIC-WIND-240724/4787
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38055	O-MIC-WIND-240724/4788
N/A	09-Jul-2024	5.5	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID: CVE-2024-38056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38056	O-MIC-WIND-240724/4789
N/A	09-Jul-2024	5.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID: CVE-2024-38017**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38017	O-MIC-WIND-240724/4790
N/A	09-Jul-2024	5.3	Windows iSCSI Service Denial of Service Vulnerability **CVE ID: CVE-2024-35270**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35270	O-MIC-WIND-240724/4791
N/A	09-Jul-2024	4.7	Windows Remote Access Connection Manager Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30071	O-MIC-WIND-240724/4792

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-30071		
Affected Version(s): * Up to (including) 10.0.25398.1009					
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37989**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37989	O-MIC-WIND-240724/4793
Product: windows_server_23h2					
Affected Version(s): * Up to (excluding) 10.0.25398.1009					
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37987**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37987	O-MIC-WIND-240724/4794
N/A	09-Jul-2024	8	Secure Boot Security Feature Bypass Vulnerability **CVE ID: CVE-2024-37988**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37988	O-MIC-WIND-240724/4795
Vendor: Mitsubishielectric					
Product: mrzjw3-mc2-utl_firmware					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	O-MIT-MRZJ-240724/4796

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	O-MIT-MRZJ-240724/4797
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	O-MIT-MRZJ-240724/4798
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	O-MIT-MRZJ-240724/4799
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges	N/A	O-MIT-MRZJ-240724/4800

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 execute arbitrary code. **CVE ID: CVE-2024-26314**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	O-MIT-MRZJ-240724/4801
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	O-MIT-MRZJ-240724/4802
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	O-MIT-MRZJ-240724/4803
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local	N/A	O-MIT-MRZJ-240724/4804

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	O-MIT-MRZJ-240724/4805
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	O-MIT-MRZJ-240724/4806
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	O-MIT-MRZJ-240724/4807
Product: sw0dnc-mneth-b_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
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	O-MIT-SW0D-240724/4808
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	O-MIT-SW0D-240724/4809
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	O-MIT-SW0D-240724/4810
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges	N/A	O-MIT-SW0D-240724/4811

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 execute arbitrary code. **CVE ID: CVE-2024-25088**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	O-MIT-SW0D-240724/4812
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	O-MIT-SW0D-240724/4813
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	O-MIT-SW0D-240724/4814
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0	N/A	O-MIT-SW0D-240724/4815

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 cause a Windows blue screen error. **CVE ID: CVE-2024-22102**		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	O-MIT-SW0D-240724/4816
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	O-MIT-SW0D-240724/4817
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	O-MIT-SW0D-240724/4818

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	O-MIT-SW0D-240724/4819
Product: sw1dnc-ccbd2-b_firmware					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	O-MIT-SW1D-240724/4820
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	O-MIT-SW1D-240724/4821
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local	N/A	O-MIT-SW1D-240724/4822

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	O-MIT-SW1D-240724/4823
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	O-MIT-SW1D-240724/4824
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	O-MIT-SW1D-240724/4825
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver	N/A	O-MIT-SW1D-240724/4826

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	O-MIT-SW1D-240724/4827
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	O-MIT-SW1D-240724/4828
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	N/A	O-MIT-SW1D-240724/4829

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-22104		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	O-MIT-SW1D-240724/4830
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	O-MIT-SW1D-240724/4831
Product: sw1dnc-ccief-b_firmware					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	O-MIT-SW1D-240724/4832
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to	N/A	O-MIT-SW1D-240724/4833

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	O-MIT-SW1D-240724/4834
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	O-MIT-SW1D-240724/4835
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	O-MIT-SW1D-240724/4836

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	O-MIT-SW1D-240724/4837
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	O-MIT-SW1D-240724/4838
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	O-MIT-SW1D-240724/4839
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	N/A	O-MIT-SW1D-240724/4840

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-22103		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	O-MIT-SW1D-240724/4841
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	O-MIT-SW1D-240724/4842
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	O-MIT-SW1D-240724/4843
Product: sw1dnc-ccief-j_firmware					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local	N/A	O-MIT-SW1D-240724/4844

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**		
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	O-MIT-SW1D-240724/4845
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	O-MIT-SW1D-240724/4846
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	O-MIT-SW1D-240724/4847

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	O-MIT-SW1D-240724/4848
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	O-MIT-SW1D-240724/4849
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	O-MIT-SW1D-240724/4850
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error.	N/A	O-MIT-SW1D-240724/4851

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-22102		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	O-MIT-SW1D-240724/4852
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	O-MIT-SW1D-240724/4853
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	O-MIT-SW1D-240724/4854
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a	N/A	O-MIT-SW1D-240724/4855

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Windows blue screen error. **CVE ID: CVE-2024-25087**		
Product: sw1dnc-mnetg-b_firmware					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	O-MIT-SW1D-240724/4856
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	O-MIT-SW1D-240724/4857
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	O-MIT-SW1D-240724/4858

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	O-MIT-SW1D-240724/4859
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	O-MIT-SW1D-240724/4860
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	O-MIT-SW1D-240724/4861
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	N/A	O-MIT-SW1D-240724/4862

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2023-51778		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	O-MIT-SW1D-240724/4863
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	O-MIT-SW1D-240724/4864
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	O-MIT-SW1D-240724/4865
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a	N/A	O-MIT-SW1D-240724/4866

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Windows blue screen error. **CVE ID: CVE-2024-22105**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	O-MIT-SW1D-240724/4867
Product: sw1dnc-qsccf-b_firmware					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	O-MIT-SW1D-240724/4868
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	O-MIT-SW1D-240724/4869

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	O-MIT-SW1D-240724/4870
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	O-MIT-SW1D-240724/4871
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-26314**	N/A	O-MIT-SW1D-240724/4872
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error.	N/A	O-MIT-SW1D-240724/4873

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
			CVE ID: CVE-2023-51777		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	O-MIT-SW1D-240724/4874
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	O-MIT-SW1D-240724/4875
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**	N/A	O-MIT-SW1D-240724/4876
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a	N/A	O-MIT-SW1D-240724/4877

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
			Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	O-MIT-SW1D-240724/4878
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	O-MIT-SW1D-240724/4879
Product: sw1dnd-emsdk-b_firmware					
Affected Version(s): *					
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2023-51776**	N/A	O-MIT-SW1D-240724/4880

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS). **CVE ID: CVE-2024-22106**	N/A	O-MIT-SW1D-240724/4881
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25086**	N/A	O-MIT-SW1D-240724/4882
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code. **CVE ID: CVE-2024-25088**	N/A	O-MIT-SW1D-240724/4883
N/A	02-Jul-2024	7.8	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges	N/A	O-MIT-SW1D-240724/4884

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 execute arbitrary code. **CVE ID: CVE-2024-26314**		
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2023-51777**	N/A	O-MIT-SW1D-240724/4885
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2023-51778**	N/A	O-MIT-SW1D-240724/4886
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22102**	N/A	O-MIT-SW1D-240724/4887
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local	N/A	O-MIT-SW1D-240724/4888

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22103**		
Out-of-bounds Write	02-Jul-2024	5.5	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS). **CVE ID: CVE-2024-22104**	N/A	O-MIT-SW1D-240724/4889
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-22105**	N/A	O-MIT-SW1D-240724/4890
N/A	02-Jul-2024	5.5	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error. **CVE ID: CVE-2024-25087**	N/A	O-MIT-SW1D-240724/4891
Vendor: Netbsd					
Product: netbsd					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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) 10.0.0					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	O-NET-NETB-240724/4892
Vendor: nuvoton					
Product: npcm705r_firmware					
Affected Version(s): * Up to (excluding) 10.10.19					
Improper Authentication	11-Jul-2024	6.7	Nuvoton - CWE-305: Authentication Bypass by Primary Weakness An attacker with write access to the SPI-Flash on an NPCM7xx BMC subsystem that uses the Nuvoton BootBlock reference code can modify the u-boot image header on	N/A	O-NUV-NPCM-240724/4893

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			flash parsed by the BootBlock which could lead to arbitrary code execution. **CVE ID: CVE-2024-38433**		
Product: npcm710r_firmware					
Affected Version(s): * Up to (excluding) 10.10.19					
Improper Authentication	11-Jul-2024	6.7	Nuvoton - CWE-305: Authentication Bypass by Primary Weakness An attacker with write access to the SPI-Flash on an NPCM7xx BMC subsystem that uses the Nuvoton BootBlock reference code can modify the u-boot image header on flash parsed by the BootBlock which could lead to arbitrary code execution. **CVE ID: CVE-2024-38433**	N/A	O-NUV-NPCM-240724/4894
Product: npcm730r_firmware					
Affected Version(s): * Up to (excluding) 10.10.19					

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 Authentication	11-Jul-2024	6.7	Nuvoton - CWE-305: Authentication Bypass by Primary Weakness An attacker with write access to the SPI-Flash on an NPCM7xx BMC subsystem that uses the Nuvoton BootBlock reference code can modify the u-boot image header on flash parsed by the BootBlock which could lead to arbitrary code execution. **CVE ID: CVE-2024-38433**	N/A	O-NUV-NPCM-240724/4895
Product: npcm750r_firmware					
Affected Version(s): * Up to (excluding) 10.10.19					
Improper Authentication	11-Jul-2024	6.7	Nuvoton - CWE-305: Authentication Bypass by Primary Weakness An attacker with write access to the SPI-Flash on an NPCM7xx BMC subsystem that uses the Nuvoton BootBlock	N/A	O-NUV-NPCM-240724/4896

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reference code can modify the u-boot image header on flash parsed by the BootBlock which could lead to arbitrary code execution. **CVE ID: CVE-2024-38433**		
Vendor: Qualcomm					
Product: 205_mobile_platform_firmware					
Affected Version(s): -					
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-205_-240724/4897
Product: 215_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-215_-240724/4898
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-215_-240724/4899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-23373	2024-bulletin.html	
Product: 315_5g_iot_modem_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-315_-240724/4900
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-315_-240724/4901
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-315_-240724/4902
Product: 9205_lte_modem_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-9205-240724/4903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-9205-240724/4904
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-9205-240724/4905
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-9205-240724/4906
Product: apq5053-aa_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-APQ5-240724/4907
Product: apq8017_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-APQ8-240724/4908

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21461		
Product: apq8037_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-APQ8-240724/4909
Product: apq8053-aa_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-APQ8-240724/4910
Product: apq8053-ac_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-APQ8-240724/4911
Product: apq8064au_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-APQ8-240724/4912

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 is freed by keymaster. **CVE ID: CVE-2024-21461**	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-APQ8-240724/4913
Product: aqt1000_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-AQT1-240724/4914
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-AQT1-240724/4915
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-AQT1-240724/4916
Buffer Copy without	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicres	O-QUA-AQT1-240724/4917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	ources/security bulletin/july-2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-AQT1-240724/4918
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-AQT1-240724/4919
Product: ar8031_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-AR80-240724/4920
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-AR80-240724/4921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-AR80-240724/4922
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-AR80-240724/4923
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-AR80-240724/4924
Product: ar8035_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-AR80-240724/4925
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-AR80-240724/4926

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-AR80-240724/4927
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-AR80-240724/4928
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-AR80-240724/4929
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-AR80-240724/4930
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-AR80-240724/4931
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-AR80-240724/4932

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
			CVE ID: CVE-2024-21462	bulletin/july-2024-bulletin.html	
Product: ar9380_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-AR93-240724/4933
Product: c-v2x_9150_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-C-V2-240724/4934
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-C-V2-240724/4935
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-C-V2-240724/4936
Product: csr8811_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): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSR8-240724/4937
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSR8-240724/4938
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSR8-240724/4939
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSR8-240724/4940
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSR8-240724/4941

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: csra6620_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSRA-240724/4942
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSRA-240724/4943
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSRA-240724/4944
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSRA-240724/4945
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSRA-240724/4946

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSRA-240724/4947
Product: csra6640_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSRA-240724/4948
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSRA-240724/4949
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSRA-240724/4950
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSRA-240724/4951

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
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSRA-240724/4952
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSRA-240724/4953
Product: csrb31024_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSRB-240724/4954
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSRB-240724/4955
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-CSRB-240724/4956

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: fastconnect_6200_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4957
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4958
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4959
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4960
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-23372		
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4962
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4963
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4964
Product: fastconnect_6700_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4965
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-FAST-240724/4966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4967
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4968
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4969
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4970
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-FAST-240724/4971

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4972
Product: fastconnect_6800_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4973
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4974
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4975
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4976

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')					
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4977
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4978
Product: fastconnect_6900_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4979
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4980
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-FAST-240724/4981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4982
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4983
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4984
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4985
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-FAST-240724/4986

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			one chunk in virtual address space. **CVE ID: CVE-2024-21460**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4987
Product: fastconnect_7800_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4988
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4989
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4990
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-FAST-240724/4991

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
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4992
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4993
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4994
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4995
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-FAST-240724/4996

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4997
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4998
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FAST-240724/4999
Product: flight_rb5_5g_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FLIG-240724/5000
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-FLIG-240724/5001

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21465	2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FLIG-240724/5002
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FLIG-240724/5003
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FLIG-240724/5004
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FLIG-240724/5005
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-FLIG-240724/5006

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FLIG-240724/5007
Product: fsm10055_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FSM1-240724/5008
Product: fsm10056_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FSM1-240724/5009
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FSM1-240724/5010
Buffer Copy without	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicres	O-QUA-FSM1-240724/5011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FSM1-240724/5012
Product: fsm20055_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FSM2-240724/5013
Product: fsm20056_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-FSM2-240724/5014
Product: home_hub_100_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC	https://docs.qualcomm.com/product/publicres	O-QUA-HOME-240724/5015

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	ources/security bulletin/july-2024-bulletin.html	
Product: immersive_home_214_platform_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5016
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5017
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5018
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5019

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: immersive_home_216_platform_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5020
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5021
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5022
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5023
Product: immersive_home_316_platform_firmware					
Affected Version(s): -					
Improper Restriction of	01-Jul-2024	7.8	Memory corruption during the secure boot process, when	https://docs.qualcomm.com/product/publicres	O-QUA-IMME-240724/5024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	ources/security bulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5025
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5026
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5027
Product: immersive_home_318_platform_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the kernel/rootfs image. **CVE ID: CVE-2024-21482**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5029
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5030
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5031
Product: immersive_home_3210_platform_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5033
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5034
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5035
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5036
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5037
Product: immersive_home_326_platform_firmware					
Affected Version(s): -					
Improper Restriction	01-Jul-2024	7.8	Memory corruption during the secure	https://docs.qualcomm.com/pr	O-QUA-IMME-240724/5038

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Operations within the Bounds of a Memory Buffer			boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	oduct/publicresources/securitybulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5039
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5040
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5041
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5042

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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IMME-240724/5043
Product: ipq4018_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ4-240724/5044
Product: ipq4019_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ4-240724/5045
Product: ipq4028_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ4-240724/5046

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: ipq4029_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ4-240724/5047
Product: ipq5010_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5048
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5049
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5050

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5051
Product: ipq5028_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5052
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5053
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5054
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-IPQ5-240724/5055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21458	2024-bulletin.html	
Product: ipq5300_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5056
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5057
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5058
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5059
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5060

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
Product: ipq5302_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5061
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5062
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5063
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5064
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-IPQ5-240724/5065

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21466	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5066
Product: ipq5312_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5067
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5068
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5069
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while	https://docs.qualcomm.com/product/publicres	O-QUA-IPQ5-240724/5070

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
			handling SA query action frame. **CVE ID: CVE-2024-21458**	ources/security bulletin/july-2024-bulletin.html	
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5071
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5072
Product: ipq5332_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5073
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5074

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5075
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5076
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5077
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ5-240724/5078
Product: ipq6000_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5079

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5080
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5081
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5082
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5083
Product: ipq6005_firmware					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5084
Product: ipq6010_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
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5085
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5086
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5087
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5088
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5089
Product: ipq6018_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): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5090
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5091
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5092
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5093
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5094

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: ipq6028_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5095
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5096
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5097
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ6-240724/5098
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-IPQ6-240724/5099

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
				2024-bulletin.html	
Product: ipq8064_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5100
Product: ipq8065_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5101
Product: ipq8068_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5102
Product: ipq8070a_firmware					
Affected Version(s): -					
Improper Restriction of	01-Jul-2024	7.8	Memory corruption during the secure boot process, when	https://docs.qualcomm.com/product/publicres	O-QUA-IPQ8-240724/5103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	ources/security bulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5104
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5105
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5106
Product: ipq8070_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')					
Product: ipq8071a_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5108
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5109
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5110
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5111
Product: ipq8072a_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
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5112
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5113
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5114
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5115
Product: ipq8074a_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-IPQ8-240724/5116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5117
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5118
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5119
Product: ipq8076a_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5120

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5121
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5122
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5123
Product: ipq8076_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5124
Buffer Copy without Checking Size of Input	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-IPQ8-240724/5125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5126
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5127
Product: ipq8078a_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5128
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5129

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5130
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5131
Product: ipq8078_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5132
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5133
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-IPQ8-240724/5134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21457	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5135
Product: ipq8173_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5136
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5137
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5138
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while	https://docs.qualcomm.com/product/publicres	O-QUA-IPQ8-240724/5139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling SA query action frame. **CVE ID: CVE-2024-21458**	ources/security bulletin/july-2024-bulletin.html	
Product: ipq8174_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5140
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5141
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5142
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ8-240724/5143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ipq9008_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5144
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5145
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5146
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5147
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-IPQ9-240724/5148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21466	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5149
Product: ipq9554_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5150
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5151
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5152
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while	https://docs.qualcomm.com/product/publicres	O-QUA-IPQ9-240724/5153

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling SA query action frame. **CVE ID: CVE-2024-21458**	ources/security bulletin/july-2024-bulletin.html	
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5154
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5155
Product: ipq9570_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5156
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5157

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5158
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5159
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5160
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5161
Product: ipq9574_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5162

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5163
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5164
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5165
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5166
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-IPQ9-240724/5167
Product: mdm9205s_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing	https://docs.qualcomm.com/pr	O-QUA-MDM9-240724/5168

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	oduct/publicresources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/security bulletin/july-2024-bulletin.html	O-QUA-MDM9-240724/5169
Product: mdm9628_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/security bulletin/july-2024-bulletin.html	O-QUA-MDM9-240724/5170
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/security bulletin/july-2024-bulletin.html	O-QUA-MDM9-240724/5171
Product: mdm9640_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/security bulletin/july-	O-QUA-MDM9-240724/5172

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21461	2024-bulletin.html	
Product: mdm9650_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-MDM9-240724/5173
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-MDM9-240724/5174
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-MDM9-240724/5175
Product: msm8996au_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-MSM8-240724/5176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-MSM8-240724/5177
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-MSM8-240724/5178
Product: pm8937_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-PM89-240724/5179
Product: pmp8074_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-PMP8-240724/5180
Product: qam8255p_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5181
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5182
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5183
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5184
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5185

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5186
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5187
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5188
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5189
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5190
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QAM8-240724/5191

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
				2024-bulletin.html	
Product: qam8295p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5192
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5193
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5194
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5195
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QAM8-240724/5196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			greater than expected size. **CVE ID: CVE-2024-23372**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5197
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5198
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5199
Product: qam8620p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5200
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QAM8-240724/5201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	bulletin/july-2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5202
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5203
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5204
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5205
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QAM8-240724/5206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-23380	2024-bulletin.html	
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5207
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5208
Product: qam8650p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5209
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5210
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5212
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5213
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5214
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5215
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5216

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5217
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5218
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5219
Product: qam8775p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5220
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5222
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5223
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5224
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5225
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5226

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5227
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5228
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5229
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAM8-240724/5230
Product: qamsrv1h_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5231

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5232
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5233
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5234
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5235
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5236

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5237
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5238
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5239
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5240
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5241
Product: qamsrv1m_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QAMS-240724/5242

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 is freed by keymaster. **CVE ID: CVE-2024-21461**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5243
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5244
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5245
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5246
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QAMS-240724/5247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5248
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5249
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5250
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5251
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QAMS-240724/5252
Product: qca0000_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): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA0-240724/5253
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA0-240724/5254
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA0-240724/5255
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA0-240724/5256
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA0-240724/5257
Product: qca4004_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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA4-240724/5258
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA4-240724/5259
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA4-240724/5260
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA4-240724/5261
Product: qca4024_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA4-240724/5262

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21482		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA4-240724/5263
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA4-240724/5264
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA4-240724/5265
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA4-240724/5266
Product: qca6174a_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5267

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21461		
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5268
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5269
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5270
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5271
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5272
Product: qca6234_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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5273
Product: qca6310_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5274
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5275
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5276
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5277

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')					
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5278
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5279
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5280
Product: qca6320_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5281
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCA6-240724/5282

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5283
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5284
Product: qca6335_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5285
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5286
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCA6-240724/5287

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5288
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5289
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5290
Product: qca6391_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5291
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCA6-240724/5292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5293
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5294
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5295
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5296
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCA6-240724/5297

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5298
Product: qca6420_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5299
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5300
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5301
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5302

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')					
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5303
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5304
Product: qca6421_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5305
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5306
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCA6-240724/5307

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21469	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5308
Product: qca6426_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5309
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5310
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5311
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5312

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')					
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5313
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5314
Product: qca6430_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5315
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5316
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCA6-240724/5317

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5318
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5319
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5320
Product: qca6431_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5321
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCA6-240724/5322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5323
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5324
Product: qca6436_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5325
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5326
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5328
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5329
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5330
Product: qca6554a_firmware					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5331
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5332

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5333
Product: qca6564au_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5334
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5335
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5336
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5337

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5338
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5339
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5340
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5341
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5342
Product: qca6564a_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC	https://docs.qualcomm.com/product/publicres	O-QUA-QCA6-240724/5343

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5344
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5345
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5346
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5347
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCA6-240724/5348

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: qca6564_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5349
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5350
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5351
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5352
Product: qca6574au_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC	https://docs.qualcomm.com/product/publicres	O-QUA-QCA6-240724/5353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5354
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5355
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5356
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5357
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCA6-240724/5358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	bulletin/july-2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5359
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5360
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5361
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5362
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5363
Product: qca6574a_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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5364
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5365
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5366
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5367
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5368

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5369
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5370
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5371
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5372
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5373
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCA6-240724/5374

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: qca6574_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5375
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5376
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5377
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5378
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCA6-240724/5379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			greater than expected size. **CVE ID: CVE-2024-23372**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5380
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5381
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5382
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5383
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5384

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5385
Product: qca6584au_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5386
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5387
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5388
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5390
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5391
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5392
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5393
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5394
Product: qca6595au_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC	https://docs.qualcomm.com/product/publicres	O-QUA-QCA6-240724/5395

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5396
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5397
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5398
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5399
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCA6-240724/5400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	bulletin/july-2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5401
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5402
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5403
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5404
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5405
Product: qca6595_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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5406
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5407
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5408
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5409
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5410

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5411
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5412
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5413
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5414
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5415
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCA6-240724/5416

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: qca6678aq_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5417
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5418
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5419
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5420
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCA6-240724/5421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			greater than expected size. **CVE ID: CVE-2024-23372**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5422
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5423
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5424
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5425
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5426

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5427
Product: qca6688aq_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5428
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5429
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5430
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5431

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5432
Product: qca6696_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5433
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5434
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5435
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5436

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5437
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5438
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5439
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5440
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5441
Integer Underflow (Wrap or	01-Jul-2024	7.5	Information disclosure while parsing sub-IE	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCA6-240724/5442

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			length during new IE generation. **CVE ID: CVE-2024-21466**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5443
Product: qca6698aq_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5444
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5445
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5446
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCA6-240724/5447

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5448
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5449
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5450
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5451
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCA6-240724/5452

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
				2024-bulletin.html	
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5453
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5454
Product: qca6797aq_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5455
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5456
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5458
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5459
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5460
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5461
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA6-240724/5462
Product: qca7500_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): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA7-240724/5463
Product: qca8072_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5464
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5465
Product: qca8075_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5466

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21482		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5467
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5468
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5469
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5470
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5471
Product: qca8081_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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5472
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5473
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5474
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5475
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')					
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5477
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5478
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5479
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5480
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5481
Product: qca8082_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
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5482
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5483
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5484
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5485
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5486

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5487
Product: qca8084_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5488
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5489
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5490
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCA8-240724/5491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21458	2024-bulletin.html	
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5492
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5493
Product: qca8085_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5494
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5496
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5497
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5498
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5499
Product: qca8337_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5500

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
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5501
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5502
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5503
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5504
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5505
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCA8-240724/5506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling SA query action frame. **CVE ID: CVE-2024-21458**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5507
Product: qca8386_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5508
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5509
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5510

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
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5511
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5512
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA8-240724/5513
Product: qca9367_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5514
Product: qca9377_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCA9-240724/5515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21461	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5516
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5517
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5518
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5519
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5520
Product: qca9379_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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5521
Product: qca9880_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5522
Product: qca9886_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5523
Product: qca9888_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			the kernel/rootfs image. **CVE ID: CVE-2024-21482**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5525
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5526
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5527
Product: qca9889_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5528

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5529
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5530
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5531
Product: qca9898_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5532
Product: qca9980_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCA9-240724/5533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Product: qca9984_firmware					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5534
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5535
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5536
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5537
Product: qca9985_firmware					
Affected Version(s): -					
Buffer Copy	01-Jul-2024	7.8	Memory corruption when allocating	https://docs.qualcomm.com/pr	O-QUA-QCA9-240724/5538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	oduct/publicresources/security bulletin/july-2024-bulletin.html	
Product: qca9990_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/security bulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5539
Product: qca9992_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/security bulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5540
Product: qca9994_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/security bulletin/july-2024-bulletin.html	O-QUA-QCA9-240724/5541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcc2073_firmware					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCC2-240724/5542
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCC2-240724/5543
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCC2-240724/5544
Product: qcc2076_firmware					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCC2-240724/5545
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCC2-240724/5546

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCC2-240724/5547
Product: qcc710_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCC7-240724/5548
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCC7-240724/5549
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCC7-240724/5550
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCC7-240724/5551

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCC7-240724/5552
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCC7-240724/5553
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCC7-240724/5554
Product: qcf8000_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCF8-240724/5555
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCF8-240724/5556

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')					
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCF8-240724/5557
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCF8-240724/5558
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCF8-240724/5559
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCF8-240724/5560
Product: qcf8001_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCF8-240724/5561

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-2024-21482		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCF8-240724/5562
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCF8-240724/5563
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCF8-240724/5564
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCF8-240724/5565
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCF8-240724/5566
Product: qcm2150_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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM2-240724/5567
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM2-240724/5568
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM2-240724/5569
Product: qcm2290_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM2-240724/5570
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCM2-240724/5571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM2-240724/5572
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM2-240724/5573
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM2-240724/5574
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM2-240724/5575
Product: qcm4290_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCM4-240724/5576

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
			context is freed by keymaster. **CVE ID: CVE-2024-21461**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM4-240724/5577
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM4-240724/5578
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM4-240724/5579
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM4-240724/5580
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCM4-240724/5581

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: qcm4325_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM4-240724/5582
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM4-240724/5583
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM4-240724/5584
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM4-240724/5585
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCM4-240724/5586

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM4-240724/5587
Product: qcm4490_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM4-240724/5588
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM4-240724/5589
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM4-240724/5590
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCM4-240724/5591

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
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM4-240724/5592
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM4-240724/5593
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM4-240724/5594
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM4-240724/5595
Product: qcm5430_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCM5-240724/5596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context is freed by keymaster. **CVE ID: CVE-2024-21461**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM5-240724/5597
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM5-240724/5598
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM5-240724/5599
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM5-240724/5600
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCM5-240724/5601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM5-240724/5602
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM5-240724/5603
Product: qcm6125_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM6-240724/5604
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM6-240724/5605
Buffer Copy without Checking Size of Input	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCM6-240724/5606

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM6-240724/5607
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM6-240724/5608
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM6-240724/5609
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM6-240724/5610
Product: qcm6490_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCM6-240724/5611

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 is freed by keymaster. **CVE ID: CVE-2024-21461**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM6-240724/5612
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM6-240724/5613
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM6-240724/5614
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM6-240724/5615
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCM6-240724/5616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM6-240724/5617
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM6-240724/5618
Product: qcm8550_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM8-240724/5619
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM8-240724/5620
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCM8-240724/5621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM8-240724/5622
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM8-240724/5623
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM8-240724/5624
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM8-240724/5625
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCM8-240724/5626

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			one chunk in virtual address space. **CVE ID: CVE-2024-21460**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCM8-240724/5627
Product: qcn5021_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5628
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5629
Product: qcn5022_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5630

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21482		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5631
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5632
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5633
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5634
Product: qcn5024_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			the kernel/rootfs image. **CVE ID: CVE-2024-21482**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5636
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5637
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5638
Product: qcn5052_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5639

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5640
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5641
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5642
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5643
Product: qcn5054_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5644

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: qcn5121_firmware					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5645
Product: qcn5122_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5646
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5647
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5649
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5650
Product: qcn5124_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5651
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5652
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCN5-240724/5653

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-2024-21457	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5654
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5655
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5656
Product: qcn5152_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5657
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCN5-240724/5658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5659
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5660
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5661
Product: qcn5154_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5662
Buffer Copy without	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicres	O-QUA-QCN5-240724/5663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5664
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5665
Product: qcn5164_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5666
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5667

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
Buffer Overflow')					
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5668
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN5-240724/5669
Product: qcn6023_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5670
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5671
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while	https://docs.qualcomm.com/product/publicres	O-QUA-QCN6-240724/5672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5673
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5674
Product: qcn6024_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5675
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5676
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCN6-240724/5677

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
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5678
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5679
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5680
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5681
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCN6-240724/5682

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21458	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5683
Product: qcn6100_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5684
Product: qcn6102_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5685
Product: qcn6112_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			the kernel/rootfs image. **CVE ID: CVE-2024-21482**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5687
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5688
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5689
Product: qcn6122_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5690

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5691
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5692
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5693
Product: qcn6132_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5694
Buffer Copy without Checking Size of Input	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCN6-240724/5695

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5696
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5697
Product: qcn6224_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5698
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5699
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5700

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21469		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5701
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5702
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5703
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5704
Product: qcn6274_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5705

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
			CVE ID: CVE-2024-21461		
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5706
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5707
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5708
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5709
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5710

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5711
Product: qcn6402_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5712
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5713
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5714
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCN6-240724/5715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21458	2024-bulletin.html	
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5716
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5717
Product: qcn6412_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5718
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5719

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
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5720
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5721
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5722
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5723
Product: qcn6422_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5724

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5725
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5726
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5727
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5728
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5729
Product: qcn6432_firmware					
Affected Version(s): -					
Improper Restriction	01-Jul-2024	7.8	Memory corruption during the secure	https://docs.qualcomm.com/pr	O-QUA-QCN6-240724/5730

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Operations within the Bounds of a Memory Buffer			boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	oduct/publicresources/securitybulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5731
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5732
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5733
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5734

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN6-240724/5735
Product: qcn7606_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN7-240724/5736
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN7-240724/5737
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN7-240724/5738
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN7-240724/5739
Product: qcn9000_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
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5740
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5741
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5742
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5743
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5744

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5745
Product: qcn9001_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5746
Product: qcn9002_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5747
Product: qcn9003_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5748

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: qcn9011_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5749
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5750
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5751
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5752
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5753

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5754
Product: qcn9012_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5755
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5756
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5757
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5759
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5760
Product: qcn9013_firmware					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5761
Product: qcn9022_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5762
Buffer Copy without	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicres	O-QUA-QCN9-240724/5763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5764
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5765
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5766
Product: qcn9024_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5767
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCN9-240724/5768

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21465	bulletin/july-2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5769
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5770
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5771
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5772
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while	https://docs.qualcomm.com/product/publicres	O-QUA-QCN9-240724/5773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5774
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5775
Product: qcn9070_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5776
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5777

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5778
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5779
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5780
Product: qcn9072_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5781
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5782

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')					
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5783
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5784
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5785
Product: qcn9074_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5786
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5787

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 kernel/rootfs image. **CVE ID: CVE-2024-21482**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5788
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5789
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5790
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5791
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5792

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: qcn9100_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5793
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5794
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5795
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5796
Product: qcn9274_firmware					
Affected Version(s): -					
Improper Restriction of	01-Jul-2024	7.8	Memory corruption during the secure boot process, when	https://docs.qualcomm.com/product/publicres	O-QUA-QCN9-240724/5797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	ources/security bulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5798
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5799
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5800
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCN9-240724/5801
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCN9-240724/5802

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21462	bulletin/july-2024-bulletin.html	
Product: qcs2290_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS2-240724/5803
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS2-240724/5804
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS2-240724/5805
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS2-240724/5806
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCS2-240724/5807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS2-240724/5808
Product: qcs410_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS4-240724/5809
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS4-240724/5810
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS4-240724/5811
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCS4-240724/5812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS4-240724/5813
Product: qcs4290_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS4-240724/5814
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS4-240724/5815
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS4-240724/5816
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCS4-240724/5817

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS4-240724/5818
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS4-240724/5819
Product: qcs4490_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS4-240724/5820
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS4-240724/5821
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCS4-240724/5822

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
			bound for the same trusted application. **CVE ID: CVE-2024-21469**	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS4-240724/5823
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS4-240724/5824
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS4-240724/5825
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS4-240724/5826
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCS4-240724/5827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21462	bulletin/july-2024-bulletin.html	
Product: qcs5430_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS5-240724/5828
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS5-240724/5829
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS5-240724/5830
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS5-240724/5831
Integer Overflow or	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCS5-240724/5832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			greater than expected size. **CVE ID: CVE-2024-23372**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS5-240724/5833
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS5-240724/5834
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS5-240724/5835
Product: qcs610_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS6-240724/5836
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCS6-240724/5837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	bulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS6-240724/5838
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS6-240724/5839
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS6-240724/5840
Product: qcs6125_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS6-240724/5841
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCS6-240724/5842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			key blob passed by the user. **CVE ID: CVE-2024-21465**	bulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS6-240724/5843
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS6-240724/5844
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS6-240724/5845
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS6-240724/5846
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCS6-240724/5847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21462	bulletin/july-2024-bulletin.html	
Product: qcs6490_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS6-240724/5848
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS6-240724/5849
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS6-240724/5850
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS6-240724/5851
Integer Overflow or	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCS6-240724/5852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			greater than expected size. **CVE ID: CVE-2024-23372**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS6-240724/5853
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS6-240724/5854
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS6-240724/5855
Product: qcs7230_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS7-240724/5856
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCS7-240724/5857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	bulletin/july-2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS7-240724/5858
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS7-240724/5859
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS7-240724/5860
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS7-240724/5861
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCS7-240724/5862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-23380	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS7-240724/5863
Product: qcs8155_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS8-240724/5864
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS8-240724/5865
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS8-240724/5866
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS8-240724/5867

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: qcs8250_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS8-240724/5868
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS8-240724/5869
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS8-240724/5870
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS8-240724/5871
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS8-240724/5872

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-23372		
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS8-240724/5873
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS8-240724/5874
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS8-240724/5875
Product: qcs8550_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS8-240724/5876
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCS8-240724/5877

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS8-240724/5878
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS8-240724/5879
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS8-240724/5880
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS8-240724/5881
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QCS8-240724/5882

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS8-240724/5883
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QCS8-240724/5884
Product: qdu1000_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDU1-240724/5885
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDU1-240724/5886
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QDU1-240724/5887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDU1-240724/5888
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDU1-240724/5889
Product: qdu1010_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDU1-240724/5890
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDU1-240724/5891
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QDU1-240724/5892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDU1-240724/5893
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDU1-240724/5894
Product: qdu1110_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDU1-240724/5895
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDU1-240724/5896
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QDU1-240724/5897

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDU1-240724/5898
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDU1-240724/5899
Product: qdu1210_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDU1-240724/5900
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDU1-240724/5901
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QDU1-240724/5902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDU1-240724/5903
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDU1-240724/5904
Product: qdx1010_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDX1-240724/5905
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDX1-240724/5906
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QDX1-240724/5907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDX1-240724/5908
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDX1-240724/5909
Product: qdx1011_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDX1-240724/5910
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDX1-240724/5911
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QDX1-240724/5912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDX1-240724/5913
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QDX1-240724/5914
Product: qep8111_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QEP8-240724/5915
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QEP8-240724/5916
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QEP8-240724/5917

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QEP8-240724/5918
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QEP8-240724/5919
Product: qfw7114_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QFW7-240724/5920
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QFW7-240724/5921
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-QFW7-240724/5922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QFW7-240724/5923
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QFW7-240724/5924
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QFW7-240724/5925
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QFW7-240724/5926
Product: qfw7124_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QFW7-240724/5927

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21461		
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QFW7-240724/5928
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QFW7-240724/5929
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QFW7-240724/5930
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QFW7-240724/5931
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QFW7-240724/5932

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QFW7-240724/5933
Product: qrb5165m_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRB5-240724/5934
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRB5-240724/5935
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRB5-240724/5936
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRB5-240724/5937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRB5-240724/5938
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRB5-240724/5939
Product: qrb5165n_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRB5-240724/5940
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRB5-240724/5941
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRB5-240724/5942

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRB5-240724/5943
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRB5-240724/5944
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRB5-240724/5945
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRB5-240724/5946
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRB5-240724/5947
Product: qru1032_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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRU1-240724/5948
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRU1-240724/5949
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRU1-240724/5950
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRU1-240724/5951
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRU1-240724/5952
Product: qru1052_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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRU1-240724/5953
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRU1-240724/5954
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRU1-240724/5955
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRU1-240724/5956
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRU1-240724/5957
Product: qru1062_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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRU1-240724/5958
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRU1-240724/5959
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRU1-240724/5960
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRU1-240724/5961
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QRU1-240724/5962
Product: qsm8250_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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QSM8-240724/5963
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QSM8-240724/5964
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QSM8-240724/5965
Product: qsm8350_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QSM8-240724/5966
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QSM8-240724/5967

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
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QSM8-240724/5968
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QSM8-240724/5969
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QSM8-240724/5970
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QSM8-240724/5971
Product: qts110_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QTS1-240724/5972

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QTS1-240724/5973
Product: qualcomm_205_mobile_platform_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QUAL-240724/5974
Product: qualcomm_215_mobile_platform_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-QUAL-240724/5975
Product: robotics_rb3_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-ROBO-240724/5976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-ROBO-240724/5977
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-ROBO-240724/5978
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-ROBO-240724/5979
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-ROBO-240724/5980
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-ROBO-240724/5981
Product: robotics_rb5_platform_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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-ROBO-240724/5982
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-ROBO-240724/5983
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-ROBO-240724/5984
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-ROBO-240724/5985
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-ROBO-240724/5986

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-ROBO-240724/5987
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-ROBO-240724/5988
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-ROBO-240724/5989
Product: sa4150p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA41-240724/5990
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA41-240724/5991

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
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA41-240724/5992
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA41-240724/5993
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA41-240724/5994
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA41-240724/5995
Product: sa4155p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA41-240724/5996

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA41-240724/5997
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA41-240724/5998
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA41-240724/5999
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA41-240724/6000
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA41-240724/6001
Product: sa6145p_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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6002
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6003
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6004
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6005
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6006

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6007
Product: sa6150p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6008
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6009
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6010
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6012
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6013
Product: sa6155p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6014
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6015
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6016

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6017
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6018
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6019
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6020
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6021
Product: sa6155_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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6022
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6023
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6024
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6025
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA61-240724/6026
Product: sa7255p_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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA72-240724/6027
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA72-240724/6028
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA72-240724/6029
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA72-240724/6030
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA72-240724/6031

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
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA72-240724/6032
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA72-240724/6033
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA72-240724/6034
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA72-240724/6035
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA72-240724/6036
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SA72-240724/6037

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: sa7775p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA77-240724/6038
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA77-240724/6039
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA77-240724/6040
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA77-240724/6041
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SA77-240724/6042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			greater than expected size. **CVE ID: CVE-2024-23372**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA77-240724/6043
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA77-240724/6044
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA77-240724/6045
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA77-240724/6046
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA77-240724/6047

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA77-240724/6048
Product: sa8145p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6049
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6050
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6051
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6053
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6054
Product: sa8150p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6055
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6056
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6057

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6058
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6059
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6060
Product: sa8155p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6061
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6062

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
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6063
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6064
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6065
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6066
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6068
Product: sa8155_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6069
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6070
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6071
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6073
Product: sa8195p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6074
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6075
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6076
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6078
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6079
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6080
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA81-240724/6081
Product: sa8255p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA82-240724/6082

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA82-240724/6083
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA82-240724/6084
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA82-240724/6085
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA82-240724/6086
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA82-240724/6087

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA82-240724/6088
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA82-240724/6089
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA82-240724/6090
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA82-240724/6091
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA82-240724/6092
Product: sa8295p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SA82-240724/6093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context is freed by keymaster. **CVE ID: CVE-2024-21461**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA82-240724/6094
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA82-240724/6095
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA82-240724/6096
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA82-240724/6097
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SA82-240724/6098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA82-240724/6099
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA82-240724/6100
Product: sa8530p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA85-240724/6101
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA85-240724/6102
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SA85-240724/6103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA85-240724/6104
Product: sa8540p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA85-240724/6105
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA85-240724/6106
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA85-240724/6107
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SA85-240724/6108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA85-240724/6109
Product: sa8620p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6110
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6111
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6112
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SA86-240724/6113

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6114
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6115
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6116
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6117
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SA86-240724/6118

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6119
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6120
Product: sa8650p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6121
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6122
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6123

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6124
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6125
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6126
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6127
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6128

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6129
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6130
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA86-240724/6131
Product: sa8770p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6132
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6133

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6134
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6135
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6136
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6137
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6138

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6139
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6140
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6141
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6142
Product: sa8775p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6143

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
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6144
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6145
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6146
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6147
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6148

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6149
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6150
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6151
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6152
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA87-240724/6153
Product: sa9000p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SA90-240724/6154

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 is freed by keymaster. **CVE ID: CVE-2024-21461**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA90-240724/6155
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA90-240724/6156
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA90-240724/6157
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA90-240724/6158
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SA90-240724/6159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA90-240724/6160
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA90-240724/6161
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA90-240724/6162
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA90-240724/6163
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SA90-240724/6164
Product: sc7180-ac_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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC71-240724/6165
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC71-240724/6166
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC71-240724/6167
Product: sc7180-ad_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC71-240724/6168
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC71-240724/6169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC71-240724/6170
Product: sc8180x-aa_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6171
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6172
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6173
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6174
Product: sc8180x-ab_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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6175
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6176
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6177
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6178
Product: sc8180x-ac_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6179

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6180
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6181
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6182
Product: sc8180x-ad_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6183
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6185
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6186
Product: sc8180x-af_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6187
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6188
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6190
Product: sc8180xp-aa_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6191
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6192
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6193
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6194
Product: sc8180xp-ab_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6195
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6196
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6197
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6198
Product: sc8180xp-ac_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6199

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6200
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6201
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6202
Product: sc8180xp-ad_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6203
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6205
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6206
Product: sc8180xp-af_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6207
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6208
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6210
Product: sc8180x\+sdx55_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6211
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC81-240724/6212
Product: sc8280xp-ab_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC82-240724/6213
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SC82-240724/6214

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC82-240724/6215
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC82-240724/6216
Product: sc8280xp-bb_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC82-240724/6217
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC82-240724/6218
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC82-240724/6219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC82-240724/6220
Product: sc8380xp_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC83-240724/6221
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC83-240724/6222
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC83-240724/6223
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SC83-240724/6224
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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD46-240724/6225
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD46-240724/6226
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD46-240724/6227
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD46-240724/6228
Product: sd626_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD62-240724/6229
Product: sd660_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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD66-240724/6230
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD66-240724/6231
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD66-240724/6232
Product: sd662_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD66-240724/6233
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SD66-240724/6234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	bulletin/july-2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD66-240724/6235
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD66-240724/6236
Product: sd670_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD67-240724/6237
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD67-240724/6238
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SD67-240724/6239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD67-240724/6240
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD67-240724/6241
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD67-240724/6242
Product: sd675_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD67-240724/6243
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SD67-240724/6244

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21465	2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD67-240724/6245
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD67-240724/6246
Product: sd730_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD73-240724/6247
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD73-240724/6248
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD73-240724/6249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')					
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD73-240724/6250
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD73-240724/6251
Product: sd820_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD82-240724/6252
Product: sd821_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD82-240724/6253
Product: sd835_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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD83-240724/6254
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD83-240724/6255
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD83-240724/6256
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD83-240724/6257
Product: sd855_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD85-240724/6258

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21461		
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD85-240724/6259
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD85-240724/6260
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD85-240724/6261
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD85-240724/6262
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD85-240724/6263
Product: sd865_5g_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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD86-240724/6264
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD86-240724/6265
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD86-240724/6266
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD86-240724/6267
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD86-240724/6268

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD86-240724/6269
Product: sd888_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD88-240724/6270
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD88-240724/6271
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD88-240724/6272
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD88-240724/6273

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-23372		
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD88-240724/6274
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD88-240724/6275
Product: sdm429w_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SDM4-240724/6276
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SDM4-240724/6277
Product: sdx55_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing	https://docs.qualcomm.com/pr	O-QUA-SDX5-240724/6278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	oduct/publicresources/securitybulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SDX5-240724/6279
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SDX5-240724/6280
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SDX5-240724/6281
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SDX5-240724/6282

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SDX5-240724/6283
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SDX5-240724/6284
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SDX5-240724/6285
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SDX5-240724/6286
Product: sdx57m_firmware					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SDX5-240724/6287
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are	https://docs.qualcomm.com/product/publicres	O-QUA-SDX5-240724/6288

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bound for the same trusted application. **CVE ID: CVE-2024-21469**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SDX5-240724/6289
Product: sdx65m_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SDX6-240724/6290
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SDX6-240724/6291
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SDX6-240724/6292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SDX6-240724/6293
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SDX6-240724/6294
Product: sdx71m_firmware					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SDX7-240724/6295
Product: sd_455_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD_4-240724/6296
Product: sd_675_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SD_6-240724/6297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context is freed by keymaster. **CVE ID: CVE-2024-21461**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD_6-240724/6298
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD_6-240724/6299
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD_6-240724/6300
Product: sd_8cx_firmware					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD_8-240724/6301
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SD_8-240724/6302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21469	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD_8-240724/6303
Product: sd_8_gen1_5g_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD_8-240724/6304
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD_8-240724/6305
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD_8-240724/6306
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD_8-240724/6307

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')					
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD_8-240724/6308
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD_8-240724/6309
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD_8-240724/6310
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SD_8-240724/6311
Product: sg4150p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SG41-240724/6312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context is freed by keymaster. **CVE ID: CVE-2024-21461**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SG41-240724/6313
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SG41-240724/6314
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SG41-240724/6315
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SG41-240724/6316
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SG41-240724/6317

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-23380	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SG41-240724/6318
Product: sg8275p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SG82-240724/6319
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SG82-240724/6320
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SG82-240724/6321
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SG82-240724/6322

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SG82-240724/6323
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SG82-240724/6324
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SG82-240724/6325
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SG82-240724/6326
Product: sm4125_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC	https://docs.qualcomm.com/product/publicres	O-QUA-SM41-240724/6327

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM41-240724/6328
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM41-240724/6329
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM41-240724/6330
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM41-240724/6331
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SM41-240724/6332

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: sm4350-ac_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM43-240724/6333
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM43-240724/6334
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM43-240724/6335
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM43-240724/6336
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SM43-240724/6337

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			greater than expected size. **CVE ID: CVE-2024-23372**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM43-240724/6338
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM43-240724/6339
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM43-240724/6340
Product: sm6150-ac_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM61-240724/6341
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SM61-240724/6342

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21465	bulletin/july-2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM61-240724/6343
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM61-240724/6344
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM61-240724/6345
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM61-240724/6346
Product: sm6225-ad_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SM62-240724/6347

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 is freed by keymaster. **CVE ID: CVE-2024-21461**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM62-240724/6348
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM62-240724/6349
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM62-240724/6350
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM62-240724/6351
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SM62-240724/6352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM62-240724/6353
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM62-240724/6354
Product: sm6250p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM62-240724/6355
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM62-240724/6356
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SM62-240724/6357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: sm6250_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM62-240724/6358
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM62-240724/6359
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM62-240724/6360
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM62-240724/6361
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SM62-240724/6362

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21462	2024-bulletin.html	
Product: sm6370_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM63-240724/6363
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM63-240724/6364
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM63-240724/6365
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM63-240724/6366
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SM63-240724/6367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM63-240724/6368
Product: sm7150-aa_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM71-240724/6369
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM71-240724/6370
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM71-240724/6371
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SM71-240724/6372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM71-240724/6373
Product: sm7150-ab_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM71-240724/6374
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM71-240724/6375
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM71-240724/6376
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SM71-240724/6377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM71-240724/6378
Product: sm7150-ac_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM71-240724/6379
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM71-240724/6380
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM71-240724/6381
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SM71-240724/6382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM71-240724/6383
Product: sm7250-aa_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6384
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6385
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6386
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SM72-240724/6387

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6388
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6389
Product: sm7250-ab_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6390
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6391
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SM72-240724/6392

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bound for the same trusted application. **CVE ID: CVE-2024-21469**	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6393
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6394
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6395
Product: sm7250-ac_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6396

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6397
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6398
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6399
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6400
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6401
Product: sm7250p_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6402
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6403
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6404
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6405
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6406

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM72-240724/6407
Product: sm7315_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6408
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6409
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6410
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6411

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-23372		
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6412
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6413
Product: sm7325-ae_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6414
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6415
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SM73-240724/6416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6417
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6418
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6419
Product: sm7325-af_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6420
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SM73-240724/6421

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21465	bulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6422
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6423
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6424
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6425
Product: sm7325p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC	https://docs.qualcomm.com/product/publicres	O-QUA-SM73-240724/6426

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6427
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6428
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6429
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM73-240724/6430
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file.	https://docs.qualcomm.com/product/publicres	O-QUA-SM73-240724/6431

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21462	ources/security bulletin/july-2024-bulletin.html	
Product: sm8150-ac_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM81-240724/6432
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM81-240724/6433
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM81-240724/6434
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM81-240724/6435
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SM81-240724/6436

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM81-240724/6437
Product: sm8250-ab_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM82-240724/6438
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM82-240724/6439
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM82-240724/6440
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SM82-240724/6441

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM82-240724/6442
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM82-240724/6443
Product: sm8250-ac_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM82-240724/6444
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM82-240724/6445
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SM82-240724/6446

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bound for the same trusted application. **CVE ID: CVE-2024-21469**	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM82-240724/6447
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM82-240724/6448
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM82-240724/6449
Product: sm8350-ac_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM83-240724/6450

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM83-240724/6451
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM83-240724/6452
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM83-240724/6453
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM83-240724/6454
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM83-240724/6455

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM83-240724/6456
Product: sm8550p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM85-240724/6457
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM85-240724/6458
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM85-240724/6459
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM85-240724/6460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM85-240724/6461
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM85-240724/6462
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM85-240724/6463
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM85-240724/6464
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SM85-240724/6465
Product: smart_audio_400_platform_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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SMAR-240724/6466
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SMAR-240724/6467
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SMAR-240724/6468
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SMAR-240724/6469
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SMAR-240724/6470

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SMAR-240724/6471
Product: snapdragon_210_processor_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6472
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6473
Product: snapdragon_212_mobile_platform_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6474
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-240724/6475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	bulletin/july-2024-bulletin.html	
Product: snapdragon_425_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6476
Product: snapdragon_427_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6477
Product: snapdragon_429_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6478
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SNAP-240724/6479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Product: snapdragon_430_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6480
Product: snapdragon_435_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6481
Product: snapdragon_439_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6482
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SNAP-240724/6483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Product: snapdragon_450_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6484
Product: snapdragon_460_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6485
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6486
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6488
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6489
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6490
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6491
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6492
Product: snapdragon_480_5g_mobile_platform_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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6493
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6494
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6495
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6496
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6497

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6498
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6499
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6500
Product: snapdragon_4_gen_1_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6501
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6502

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6503
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6504
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6505
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6506
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6508
Product: snapdragon_4_gen_2_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6509
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6510
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6511
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6512

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6513
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6514
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6515
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6516
Product: snapdragon_625_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6517

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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_626_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6518
Product: snapdragon_630_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6519
Product: snapdragon_632_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6520
Product: snapdragon_636_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6521

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21461		
Product: snapdragon_660_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6522
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6523
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6524
Product: snapdragon_662_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6525

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6526
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6527
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6528
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6529
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6530

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
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6531
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6532
Product: snapdragon_665_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6533
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6534
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6536
Product: snapdragon_670_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6537
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6538
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6539
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6540

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6541
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6542
Product: snapdragon_675_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6543
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6544
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6545

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6546
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6547
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6548
Product: snapdragon_680_4g_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6549
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6550

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6551
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6552
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6553
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6554
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6555

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6556
Product: snapdragon_690_5g_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6557
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6558
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6559
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6561
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6562
Product: snapdragon_695_5g_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6563
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6564
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6565

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6566
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6567
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6568
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6569
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6570
Product: snapdragon_710_mobile_platform_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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6571
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6572
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6573
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6574
Product: snapdragon_712_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SNAP-240724/6575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context is freed by keymaster. **CVE ID: CVE-2024-21461**	2024-bulletin.html	
Product: snapdragon_720g_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6576
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6577
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6578
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6580
Product: snapdragon_750g_5g_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6581
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6582
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6583
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6585
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6586
Product: snapdragon_778g_5g_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6587
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6588
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6589

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6590
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6591
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6592
Product: snapdragon_780g_5g_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6593
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6594

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6595
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6596
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6597
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6598
Product: snapdragon_7c\+_gen_3_compute_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SNAP-240724/6599

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21461	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6600
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6601
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6602
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6603
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SNAP-240724/6604

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: snapdragon_820_automotive_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6605
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6606
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6607
Product: snapdragon_820_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6608

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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_821_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6609
Product: snapdragon_835_mobile_pc_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6610
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6611
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6612
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-240724/6613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packets during VBO bind operation. **CVE ID: CVE-2024-23380**	ources/security bulletin/july-2024-bulletin.html	
Product: snapdragon_845_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6614
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6615
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6616
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6617
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-240724/6618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6619
Product: snapdragon_850_mobile_compute_platform_firmware					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6620
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6621
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6622
Product: snapdragon_855_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-240724/6623

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6624
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6625
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6626
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6627
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SNAP-240724/6628

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: snapdragon_865_5g_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6629
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6630
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6631
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6632
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SNAP-240724/6633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6634
Product: snapdragon_888_5g_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6635
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6636
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6637
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SNAP-240724/6638

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6639
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6640
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6641
Product: snapdragon_8\+_gen_1_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6642

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6643
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6644
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6645
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6646
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6647

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6648
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6649
Product: snapdragon_8\+_gen_2_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6650
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6651
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6652
Buffer Copy without	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-240724/6653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	ources/security bulletin/july-2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6654
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6655
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6656
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6657

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6658
Product: snapdragon_8_gen_1_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6659
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6660
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6661
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6663
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6664
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6665
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6666
Product: snapdragon_8_gen_2_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6667

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6668
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6669
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6670
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6671
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6672

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6673
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6674
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6675
Product: snapdragon_8_gen_3_mobile_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6676
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6678
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6679
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6680
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6681
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6683
Product: snapdragon_ar2_gen_1_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6684
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6685
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6686
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6687

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6688
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6689
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6690
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6691
Product: snapdragon_auto_4g_modem_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6692

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6693
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6694
Product: snapdragon_auto_5g_modem-rf_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6695
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6696
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SNAP-240724/6697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-23373	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6698
Product: snapdragon_auto_5g_modem-rf_gen_2_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6699
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6700
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6701
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')					
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6703
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6704
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6705
Product: snapdragon_w5\+_gen_1_wearable_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6706
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6707

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6708
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6709
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6710
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6711
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6712
Product: snapdragon_wear_1300_platform_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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6713
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6714
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6715
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6716
Product: snapdragon_wear_4100\+_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6717

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6718
Product: snapdragon_x12_lte_modem_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6719
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6720
Product: snapdragon_x24_lte_modem_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6721
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-240724/6722

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			key blob passed by the user. **CVE ID: CVE-2024-21465**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6723
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6724
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6725
Product: snapdragon_x35_5g_modem-rf_system_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6726
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-240724/6727

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			key blob passed by the user. **CVE ID: CVE-2024-21465**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6728
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6729
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6730
Product: snapdragon_x50_5g_modem-rf_system_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6731
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-240724/6732

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			key blob passed by the user. **CVE ID: CVE-2024-21465**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6733
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6734
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6735
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6736
Product: snapdragon_x55_5g_modem-rf_system_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-240724/6737

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6738
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6739
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6740
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6741
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SNAP-240724/6742

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: snapdragon_x62_5g_modem-rf_system_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6743
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6744
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6745
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6746
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SNAP-240724/6747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6748
Product: snapdragon_x65_5g_modem-rf_system_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6749
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6750
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6751
Improper Restriction of Operations within the	01-Jul-2024	7.8	Memory corruption during the secure boot process, when the `bootm` command is used, it	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SNAP-240724/6752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			bypasses the authentication of the kernel/rootfs image. **CVE ID: CVE-2024-21482**	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6753
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6754
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6755
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6756
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SNAP-240724/6757

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21462	2024-bulletin.html	
Product: snapdragon_x70_modem-rf_system_firmware					
Affected Version(s): -					
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6758
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6759
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6760
Product: snapdragon_x72_5g_modem-rf_system_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6761
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SNAP-240724/6762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6763
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6764
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6765
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6766
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6767
Product: snapdragon_x75_5g_modem-rf_system_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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6768
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6769
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6770
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6771
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6772
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-240724/6773

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling SA query action frame. **CVE ID: CVE-2024-21458**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6774
Product: snapdragon_xr1_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6775
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6776
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6777
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-240724/6778

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	bulletin/july-2024-bulletin.html	
Product: snapdragon_xr2\+_gen_1_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6779
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6780
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6781
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6782
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-240724/6783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6784
Product: snapdragon_xr2_5g_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6785
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6786
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6787
Buffer Copy without Checking	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-240724/6788

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	bulletin/july-2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6789
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SNAP-240724/6790
Product: srv1h_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6791
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6792
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SRV1-240724/6793

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bound for the same trusted application. **CVE ID: CVE-2024-21469**	bulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6794
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6795
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6796
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6797
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SRV1-240724/6798

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21457	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6799
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6800
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6801
Product: srv1l_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6802
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SRV1-240724/6803

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6804
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6805
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6806
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6807
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-SRV1-240724/6808

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6809
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6810
Product: srv1m_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6811
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6812
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6814
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6815
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6816
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6817
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6818

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.5	Information disclosure while handling SA query action frame. **CVE ID: CVE-2024-21458**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6819
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6820
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SRV1-240724/6821
Product: ssg2115p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SSG2-240724/6822
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SSG2-240724/6823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SSG2-240724/6824
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SSG2-240724/6825
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SSG2-240724/6826
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SSG2-240724/6827
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SSG2-240724/6828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SSG2-240724/6829
Product: ssg2125p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SSG2-240724/6830
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SSG2-240724/6831
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SSG2-240724/6832
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SSG2-240724/6833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SSG2-240724/6834
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SSG2-240724/6835
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SSG2-240724/6836
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SSG2-240724/6837
Product: sw5100p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SW51-240724/6838

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SW51-240724/6839
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SW51-240724/6840
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SW51-240724/6841
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SW51-240724/6842
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SW51-240724/6843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SW51-240724/6844
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SW51-240724/6845
Product: sw5100_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SW51-240724/6846
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SW51-240724/6847
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SW51-240724/6848

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SW51-240724/6849
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SW51-240724/6850
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SW51-240724/6851
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SW51-240724/6852
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SW51-240724/6853
Product: sxr1120_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR1-240724/6854
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR1-240724/6855
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR1-240724/6856
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR1-240724/6857
Product: sxr1230p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR1-240724/6858

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21461		
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR1-240724/6859
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR1-240724/6860
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR1-240724/6861
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR1-240724/6862
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR1-240724/6863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-23373		
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR1-240724/6864
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR1-240724/6865
Product: sxr2130_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6866
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6867
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6868

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6869
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6870
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6871
Product: sxr2230p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6872
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6873

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6874
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6875
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6876
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6877
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6878

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6879
Product: sxr2250p_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6880
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6881
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6882
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6884
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6885
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6886
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-SXR2-240724/6887
Product: talynplus_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-TALY-240724/6888

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-TALY-240724/6889
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-TALY-240724/6890
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-TALY-240724/6891
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-TALY-240724/6892
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-TALY-240724/6893

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-TALY-240724/6894
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-TALY-240724/6895
Product: video_collaboration_vc1_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6896
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6897
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6899
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6900
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6901
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6902
Product: video_collaboration_vc3_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6903

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6904
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6905
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6906
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6907
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6908

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6909
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6910
Product: video_collaboration_vc5_platform_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6911
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6912
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6913
Buffer Copy without	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicres	O-QUA-VIDE-240724/6914

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	ources/security bulletin/july-2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6915
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6916
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6917
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VIDE-240724/6918
Product: vision_intelligence_300_platform_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VISI-240724/6919
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VISI-240724/6920
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VISI-240724/6921
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VISI-240724/6922
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VISI-240724/6923
Product: vision_intelligence_400_platform_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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VISI-240724/6924
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VISI-240724/6925
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VISI-240724/6926
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VISI-240724/6927
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VISI-240724/6928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-VISI-240724/6929
Product: wcd9306_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6930
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6931
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6932
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6933
Product: wcd9326_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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6934
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6935
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6936
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6937
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6938

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6939
Product: wcd9335_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6940
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6941
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6942
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6944
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6945
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6946
Product: wcd9340_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6947
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6949
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6950
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6951
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6952
Out-of-bounds Read	01-Jul-2024	7.5	INformation disclosure while handling Multi-link IE in beacon frame. **CVE ID: CVE-2024-21457**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6953
Out-of-bounds Read	01-Jul-2024	7.5	Information disclosure while	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WCD9-240724/6954

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling SA query action frame. **CVE ID: CVE-2024-21458**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-240724/6955
Product: wcd9341_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6956
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6957
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6958
Buffer Copy without Checking Size of	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-WCD9-250724/6959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6960
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6961
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6962
Product: wcd9360_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6963
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-WCD9-250724/6964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21462	2024-bulletin.html	
Product: wcd9370_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6965
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6966
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6967
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6968
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-WCD9-250724/6969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			greater than expected size. **CVE ID: CVE-2024-23372**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6970
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6971
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6972
Product: wcd9371_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6973
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WCD9-250724/6974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21465	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6975
Product: wcd9375_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6976
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6977
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6978
Buffer Copy without Checking Size of Input ('Classic	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-WCD9-250724/6979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			**CVE ID: CVE-2024-23368**	2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6980
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6981
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6982
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6983
Product: wcd9380_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-WCD9-250724/6984

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 is freed by keymaster. **CVE ID: CVE-2024-21461**	2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6985
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6986
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6987
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6988
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-WCD9-250724/6989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anon buffers are getting released. **CVE ID: CVE-2024-23373**	2024-bulletin.html	
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6990
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6991
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6992
Product: wcd9385_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6993
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	O-QUA-WCD9-250724/6994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			key blob passed by the user. **CVE ID: CVE-2024-21465**	ources/security bulletin/july-2024-bulletin.html	
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6995
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6996
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6997
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/6998
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WCD9-250724/6999

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-23380	bulletin/july-2024-bulletin.html	
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/7000
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/7001
Product: wcd9390_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/7002
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/7003
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-	O-QUA-WCD9-250724/7004

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bound for the same trusted application. **CVE ID: CVE-2024-21469**	2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/7005
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/7006
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/7007
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/7008
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WCD9-250724/7009

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	bulletin/july-2024-bulletin.html	
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/7010
Product: wcd9395_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/7011
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/7012
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/7013
Buffer Copy without Checking	01-Jul-2024	7.8	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WCD9-250724/7014

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			entry in an SMEM partition. **CVE ID: CVE-2024-23368**	bulletin/july-2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/7015
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/7016
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/7017
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCD9-250724/7018
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file.	https://docs.qualcomm.com/product/publicres	O-QUA-WCD9-250724/7019

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-21462	ources/security bulletin/july-2024-bulletin.html	
Product: wcn3610_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7020
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7021
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7022
Product: wcn3615_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-21461		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7024
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7025
Product: wcn3620_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7026
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7027
Product: wcn3660b_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7028
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7029
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7030
Product: wcn3660_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7031
Product: wcn3680b_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC	https://docs.qualcomm.com/product/publicres	O-QUA-WCN3-250724/7032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	ources/security bulletin/july-2024-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7033
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7034
Product: wcn3680_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7035
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7036

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7037
Product: wcn3910_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7038
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7039
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7040
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7041

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7042
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7043
Product: wcn3950_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7044
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7045
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7046

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7047
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7048
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7049
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7050
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7051
Product: wcn3980_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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7052
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7053
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7054
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7055
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7056

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7057
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7058
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7059
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7060
Product: wcn3988_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7061

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7062
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7063
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7064
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7065
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7066

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7067
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7068
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7069
Product: wcn3990_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7070
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7072
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7073
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7074
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7075
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7076
Product: wcn3999_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
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7077
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7078
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7079
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN3-250724/7080
Product: wcn6740_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN6-250724/7081

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN6-250724/7082
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN6-250724/7083
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN6-250724/7084
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN6-250724/7085
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WCN6-250724/7086
Product: wsa8810_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

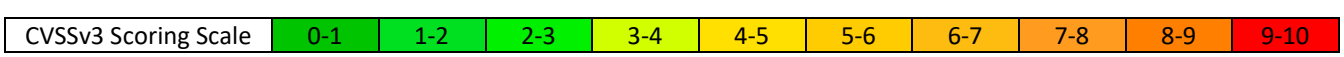
Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7087
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7088
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7089
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7090
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7091

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7092
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7093
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7094
Product: wsa8815_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7095
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7097
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7098
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7099
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7100
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7101



* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7102
Product: wsa8830_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7103
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7104
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7105
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7106

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7107
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7108
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7109
Integer Underflow (Wrap or Wraparound)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7110
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7111
Product: wsa8832_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7112
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7113
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7114
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7115
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7116

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7117
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7118
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7119
Product: wsa8835_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7120
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7121

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7122
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7123
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7124
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7125
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7126

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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)	01-Jul-2024	7.5	Information disclosure while parsing sub-IE length during new IE generation. **CVE ID: CVE-2024-21466**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7127
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7128
Product: wsa8840_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7129
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7130
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7131
Buffer Copy	01-Jul-2024	7.8	Memory corruption when allocating	https://docs.qualcomm.com/pr	O-QUA-WSA8-250724/7132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	oduct/publicresources/securitybulletin/july-2024-bulletin.html	
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7133
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7134
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7135
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7136

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7137
Product: wsa8845h_firmware					
Affected Version(s): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7138
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7139
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7140
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7141

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7142
Use After Free	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7143
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7144
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7145
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7146
Product: wsa8845_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): -					
Double Free	01-Jul-2024	7.8	Memory corruption while performing finish HMAC operation when context is freed by keymaster. **CVE ID: CVE-2024-21461**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7147
Out-of-bounds Read	01-Jul-2024	7.8	Memory corruption while processing key blob passed by the user. **CVE ID: CVE-2024-21465**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7148
Out-of-bounds Write	01-Jul-2024	7.8	Memory corruption when an invoke call and a TEE call are bound for the same trusted application. **CVE ID: CVE-2024-21469**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7149
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jul-2024	7.8	Memory corruption when allocating and accessing an entry in an SMEM partition. **CVE ID: CVE-2024-23368**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7150
Integer Overflow or Wraparound	01-Jul-2024	7.8	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size. **CVE ID: CVE-2024-23372**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7151

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	01-Jul-2024	7.8	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released. **CVE ID: CVE-2024-23373**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7152
Use After Free	01-Jul-2024	7.8	Memory corruption while handling user packets during VBO bind operation. **CVE ID: CVE-2024-23380**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7153
Use of Insufficiently Random Values	01-Jul-2024	6.5	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space. **CVE ID: CVE-2024-21460**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7154
Out-of-bounds Read	01-Jul-2024	5.5	Transient DOS while loading the TA ELF file. **CVE ID: CVE-2024-21462**	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2024-bulletin.html	O-QUA-WSA8-250724/7155
Vendor: Redhat					
Product: 389_directory_server					
Affected Version(s): -					
N/A	09-Jul-2024	6.5	A flaw was found in the 389 Directory Server. This flaw allows an unauthenticated user to cause a systematic server	https://access.redhat.com/security/cve/CVE-2024-6237	O-RED-389_-250724/7156

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash while sending a specific extended search request, leading to a denial of service. **CVE ID: CVE-2024-6237**		
Product: enterprise_linux					
Affected Version(s): 8.0					
Out-of-bounds Read	05-Jul-2024	6.8	A flaw was found in the virtio-net device in QEMU. When enabling the RSS feature on the virtio-net network card, the indirections_table data within RSS becomes controllable. Setting excessively large values may cause an index out-of-bounds issue, potentially resulting in heap overflow access. This flaw allows a privileged user in the guest to crash the QEMU process on the host. **CVE ID: CVE-2024-6505**	N/A	O-RED-ENTE-250724/7157
Affected Version(s): 9.0					
Concurrent Execution using Shared Resource with Improper	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.yc	O-RED-ENTE-250724/7158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	ombinator.com/item?id=40843778	
Out-of-bounds Read	05-Jul-2024	6.8	A flaw was found in the virtio-net device in QEMU. When enabling the RSS feature on the virtio-net network card, the indirections_table data within RSS becomes controllable. Setting excessively large values may cause an index out-of-bounds issue, potentially resulting in heap overflow access. This flaw allows a privileged user in the guest to crash the QEMU process on the host. **CVE ID: CVE-2024-6505**	N/A	O-RED-ENTE-250724/7159
N/A	09-Jul-2024	6.5	A flaw was found in the 389 Directory Server. This flaw allows an unauthenticated	https://access.redhat.com/security/cve/CVE-2024-6237	O-RED-ENTE-250724/7160

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 to cause a systematic server crash while sending a specific extended search request, leading to a denial of service. **CVE ID: CVE-2024-6237**		
Product: enterprise_linux_eus					
Affected Version(s): 9.4					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	O-RED-ENTE-250724/7161
Product: enterprise_linux_for_arm_64					
Affected Version(s): 9.0_aarch64					
Concurrent Execution using Shared Resource with Improper Synchroniz	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/	O-RED-ENTE-250724/7162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	item?id=40843778	
Product: enterprise_linux_for_arm_64_eus					
Affected Version(s): 9.4_aarch64					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	O-RED-ENTE-250724/7163
Product: enterprise_linux_for_ibm_z_systems					
Affected Version(s): 9.0_s390x					
Concurrent Execution using Shared Resource	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.ht	O-RED-ENTE-250724/7164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			(sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	ml, https://news.ycombinator.com/item?id=40843778	
Product: enterprise_linux_for_ibm_z_systems_eus					
Affected Version(s): 9.4_s390x					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	O-RED-ENTE-250724/7165
Product: enterprise_linux_for_power_little_endian					
Affected Version(s): 9.0_ppc64le					
Concurrent Execution	01-Jul-2024	8.1	A security regression (CVE-	https://lists.mindrot.org/piper	O-RED-ENTE-250724/7166

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Shared Resource with Improper Synchronization ('Race Condition')			2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	mail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	
Product: enterprise_linux_for_power_little_endian_eus					
Affected Version(s): 9.4_ppc64le					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	O-RED-ENTE-250724/7167
Product: enterprise_linux_server_aus					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): 9.4					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	O-RED-ENTE-250724/7168
Vendor: rensas					
Product: arm-trusted-firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Jul-2024	6.7	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in Renesas arm-trusted-firmware allows Local Execution of Code. This vulnerability is associated with program files https://github.Com/renesas-rcar/arm-trusted-firmware/blob/rcar_gen3_v2.5/driver	https://github.com/renesas-rcar/arm-trusted-firmware/commit/235f85b654a031f7647e81b86fc8e4ffeb430164	O-REN-ARM--250724/7169

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			s/renesas/common/io/i... https://github.Com/renesas-rcar/arm-trusted-firmware/blob/rcar_gen3_v2.5/drivers/renesas/common/io/io_rcar.C . In line 313 "addr_loaded_cnt" is checked not to be "CHECK_IMAGE_AREA_CNT" (5) or larger, this check does not halt the function. Immediately after (line 317) there will be an overflow in the buffer and the value of "dst" will be written to the area immediately after the buffer, which is "addr_loaded_cnt". This will allow an attacker to freely control the value of "addr_loaded_cnt" and thus control the destination of the write immediately after (line 318). The write in line 318 will then be fully		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controlled by said attacker, with whichever address and whichever value ("len") they desire. **CVE ID: CVE-2024-6563**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Jul-2024	6.7	Buffer overflow in "rcar_dev_init" due to using due to using untrusted data (rcar_image_number) as a loop counter before verifying it against RCAR_MAX_BL3X_IMAGE. This could lead to a full bypass of secure boot. **CVE ID: CVE-2024-6564**	https://github.com/renesas-rcar/arm-trusted-firmware/commit/c9fb3558410032d2660c7f3b7d4b87dec09fe2f2	O-REN-ARM--250724/7170
Vendor: Samsung					
Product: android					
Affected Version(s): 12.0					
Improper Authentication	02-Jul-2024	8.8	Improper input validation in BLE prior to SMR Jul-2024 Release 1 allows adjacent attackers to trigger abnormal behavior. **CVE ID: CVE-2024-20890**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7171
N/A	02-Jul-2024	8.8	Improper input validation in parsing and distributing RTCP packet in librtp.so prior to SMR Jul-	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7172

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2024 Release 1 allows remote attackers to execute arbitrary code with system privilege. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34593**		
N/A	02-Jul-2024	7.8	Improper access control in OneUIHome prior to SMR Jul-2024 Release 1 allows local attackers to launch privileged activities. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-20888**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7173
N/A	02-Jul-2024	7.8	Improper access control in launchFullscreenIntent of SystemUI prior to SMR Jul-2024 Release 1 allows local attackers to launch privileged activities. **CVE ID: CVE-2024-20891**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7174
Improper Verification of Cryptograp	02-Jul-2024	7.8	Improper verification of signature in FilterProvider	https://security.samsungmobile.com/securityUpdate.smsb?yea	O-SAM-ANDR-250724/7175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
hic Signature			prior to SMR Jul-2024 Release 1 allows local attackers to execute privileged behaviors. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-20892**	r=2024&month=07	
Out-of-bounds Write	02-Jul-2024	7.8	Improper input validation in libmediaextractorservice.so prior to SMR Jul-2024 Release 1 allows local attackers to trigger memory corruption. **CVE ID: CVE-2024-20893**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7176
Out-of-bounds Write	02-Jul-2024	7.8	Improper input validation in copying data to buffer cache in libsaped prior to SMR Jul-2024 Release 1 allows local attackers to write out-of-bounds memory. **CVE ID: CVE-2024-20901**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7177
N/A	02-Jul-2024	7.8	Improper access control in launchApp of SystemUI prior to SMR Jul-2024 Release 1 allows local attackers to	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			launch privileged activities. **CVE ID: CVE-2024-34585**		
N/A	02-Jul-2024	7.8	Improper access control in clickAdapterItem of SystemUI prior to SMR Jul-2024 Release 1 allows local attackers to launch privileged activities. **CVE ID: CVE-2024-34595**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7179
N/A	02-Jul-2024	6.8	Improper input validation in parsing application information from RTCP packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to execute arbitrary code with system privilege. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34587**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7180
N/A	02-Jul-2024	6.5	Improper input validation?in parsing RTCP SR packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7181

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34588**		
N/A	02-Jul-2024	6.5	Improper input validation in parsing RTCP RR packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34589**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7182
N/A	02-Jul-2024	5.5	Improper access control in Dar service prior to SMR Jul-2024 Release 1 allows local attackers to bypass restriction for calling SDP features. **CVE ID: CVE-2024-20895**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7183
N/A	02-Jul-2024	5.5	Use of implicit intent for sensitive communication in Configuration message prior to SMR Jul-2024 Release 1 allows local attackers to	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7184

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 sensitive information. **CVE ID: CVE-2024-20896**		
N/A	02-Jul-2024	5.5	Use of implicit intent for sensitive communication in FCM function in IMS service prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information. **CVE ID: CVE-2024-20897**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7185
N/A	02-Jul-2024	5.5	Use of implicit intent for sensitive communication in SoftphoneClient in IMS service prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information. **CVE ID: CVE-2024-20898**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7186
N/A	02-Jul-2024	5.5	Use of implicit intent for sensitive communication in RCS function in IMS service prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information. **CVE ID: CVE-2024-20899**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7187

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	5.5	Exposure of sensitive information in proc file system prior to SMR Jul-2024 Release 1 allows local attackers to read kernel memory address. **CVE ID: CVE-2024-34594**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7188
N/A	08-Jul-2024	5.5	Use of implicit intent for sensitive communication in Samsung Messages prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34602**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7189
Improper Authentication	02-Jul-2024	4.3	Improper authentication in BLE prior to SMR Jul-2024 Release 1 allows adjacent attackers to pair with devices. **CVE ID: CVE-2024-20889**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7190
Improper Handling of Exceptional Conditions	02-Jul-2024	4.3	Improper handling of exceptional conditions in Secure Folder prior to SMR Jul-2024 Release 1 allows	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7191

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 bypass authentication under certain condition. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-20894**		
N/A	02-Jul-2024	4.3	Improper input validation흉in parsing an item type from RTCP SDES packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34590**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7192
N/A	02-Jul-2024	4.3	Improper input validation in parsing an item data from RTCP SDES packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7193

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			triggering this vulnerability. **CVE ID: CVE-2024-34591**		
N/A	02-Jul-2024	4.3	Improper input validation in parsing RTCP SDES packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34592**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7194
Improper Authentication	02-Jul-2024	3.3	Improper authentication in MTP application prior to SMR Jul-2024 Release 1 allows local attackers to enter MTP mode without proper authentication. **CVE ID: CVE-2024-20900**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7195
N/A	02-Jul-2024	3.3	Improper access control in system property prior to SMR Jul-2024 Release 1 allows local attackers to get device identifier.	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7196

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-34583		
N/A	02-Jul-2024	3.3	Improper access control in KnoxCustomManagerService prior to SMR Jul-2024 Release 1 allows local attackers to configure Knox privacy policy. **CVE ID: CVE-2024-34586**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7197
Affected Version(s): 14.0					
Improper Authentication	02-Jul-2024	8.8	Improper input validation in BLE prior to SMR Jul-2024 Release 1 allows adjacent attackers to trigger abnormal behavior. **CVE ID: CVE-2024-20890**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7198
N/A	02-Jul-2024	8.8	Improper input validation in parsing and distributing RTCP packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to execute arbitrary code with system privilege. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34593**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jul-2024	7.8	Improper access control in OneUIHome prior to SMR Jul-2024 Release 1 allows local attackers to launch privileged activities. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-20888**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7200
N/A	02-Jul-2024	7.8	Improper access control in launchFullscreenIntent of SystemUI prior to SMR Jul-2024 Release 1 allows local attackers to launch privileged activities. **CVE ID: CVE-2024-20891**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7201
Improper Verification of Cryptographic Signature	02-Jul-2024	7.8	Improper verification of signature in FilterProvider prior to SMR Jul-2024 Release 1 allows local attackers to execute privileged behaviors. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-20892**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7202

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-Jul-2024	7.8	Improper input validation in libmediaextractorservice.so prior to SMR Jul-2024 Release 1 allows local attackers to trigger memory corruption. **CVE ID: CVE-2024-20893**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7203
Out-of-bounds Write	02-Jul-2024	7.8	Improper input validation in copying data to buffer cache in libsaped prior to SMR Jul-2024 Release 1 allows local attackers to write out-of-bounds memory. **CVE ID: CVE-2024-20901**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7204
N/A	02-Jul-2024	7.8	Improper access control in launchApp of SystemUI prior to SMR Jul-2024 Release 1 allows local attackers to launch privileged activities. **CVE ID: CVE-2024-34585**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7205
N/A	02-Jul-2024	7.8	Improper access control in clickAdapterItem of SystemUI prior to SMR Jul-2024 Release 1 allows local attackers to	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7206

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			launch privileged activities. **CVE ID: CVE-2024-34595**		
N/A	02-Jul-2024	6.8	Improper input validation in parsing application information from RTCP packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to execute arbitrary code with system privilege. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34587**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7207
N/A	02-Jul-2024	6.5	Improper input validation?in parsing RTCP SR packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34588**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7208
N/A	02-Jul-2024	6.5	Improper input validation in parsing RTCP RR packet in librtp.so	https://security.samsungmobile.com/securityUpdate.smsb?yea	O-SAM-ANDR-250724/7209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34589**	r=2024&month=07	
N/A	02-Jul-2024	5.5	Improper access control in Dar service prior to SMR Jul-2024 Release 1 allows local attackers to bypass restriction for calling SDP features. **CVE ID: CVE-2024-20895**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7210
N/A	02-Jul-2024	5.5	Use of implicit intent for sensitive communication in Configuration message prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information. **CVE ID: CVE-2024-20896**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7211
N/A	02-Jul-2024	5.5	Use of implicit intent for sensitive communication in FCM function in IMS service prior to SMR Jul-2024 Release 1 allows	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7212

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attackers to get sensitive information. **CVE ID: CVE-2024-20897**		
N/A	02-Jul-2024	5.5	Use of implicit intent for sensitive communication in SoftphoneClient in IMS service prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information. **CVE ID: CVE-2024-20898**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7213
N/A	02-Jul-2024	5.5	Use of implicit intent for sensitive communication in RCS function in IMS service prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information. **CVE ID: CVE-2024-20899**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7214
N/A	02-Jul-2024	5.5	Exposure of sensitive information in proc file system prior to SMR Jul-2024 Release 1 allows local attackers to read kernel memory address. **CVE ID: CVE-2024-34594**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7215

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	08-Jul-2024	5.5	Use of implicit intent for sensitive communication in Samsung Messages prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34602**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7216
N/A	08-Jul-2024	5.5	Improper access control in Samsung Message prior to SMR Jul-2024 Release 1 allows local attackers to access location data. **CVE ID: CVE-2024-34603**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7217
Improper Authentication	02-Jul-2024	4.3	Improper authentication in BLE prior to SMR Jul-2024 Release 1 allows adjacent attackers to pair with devices. **CVE ID: CVE-2024-20889**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7218
Improper Handling of Exceptional Conditions	02-Jul-2024	4.3	Improper handling of exceptional conditions in Secure Folder prior to SMR Jul-2024 Release 1 allows physical attackers	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7219

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 bypass authentication under certain condition. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-20894**		
N/A	02-Jul-2024	4.3	Improper input validation in parsing an item type from RTCP SDES packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34590**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7220
N/A	02-Jul-2024	4.3	Improper input validation in parsing an item data from RTCP SDES packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability.	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7221

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-34591		
N/A	02-Jul-2024	4.3	Improper input validation in parsing RTCP SDES packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34592**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7222
Improper Authentication	02-Jul-2024	3.3	Improper authentication in MTP application prior to SMR Jul-2024 Release 1 allows local attackers to enter MTP mode without proper authentication. **CVE ID: CVE-2024-20900**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7223
N/A	02-Jul-2024	3.3	Improper access control in system property prior to SMR Jul-2024 Release 1 allows local attackers to get device identifier. **CVE ID: CVE-2024-34583**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7224

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	3.3	Improper access control in KnoxCustomManagerService prior to SMR Jul-2024 Release 1 allows local attackers to configure Knox privacy policy. **CVE ID: CVE-2024-34586**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7225
Affected Version(s): 13.0					
Improper Authentication	02-Jul-2024	8.8	Improper input validation in BLE prior to SMR Jul-2024 Release 1 allows adjacent attackers to trigger abnormal behavior. **CVE ID: CVE-2024-20890**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7226
N/A	02-Jul-2024	8.8	Improper input validation in parsing and distributing RTCP packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to execute arbitrary code with system privilege. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34593**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7227
N/A	02-Jul-2024	7.8	Improper access control in OneUIHome prior	https://security.samsungmobile.com/securityU	O-SAM-ANDR-250724/7228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to SMR Jul-2024 Release 1 allows local attackers to launch privileged activities. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-20888**	pdate.smsb?year=2024&month=07	
N/A	02-Jul-2024	7.8	Improper access control in launchFullscreenIntent of SystemUI prior to SMR Jul-2024 Release 1 allows local attackers to launch privileged activities. **CVE ID: CVE-2024-20891**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7229
Improper Verification of Cryptographic Signature	02-Jul-2024	7.8	Improper verification of signature in FilterProvider prior to SMR Jul-2024 Release 1 allows local attackers to execute privileged behaviors. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-20892**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7230
Out-of-bounds Write	02-Jul-2024	7.8	Improper input validation in libmediaextractors	https://security.samsungmobile.com/securityU	O-SAM-ANDR-250724/7231

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ervice.so prior to SMR Jul-2024 Release 1 allows local attackers to trigger memory corruption. **CVE ID: CVE-2024-20893**	pdate.smsb?year=2024&month=07	
Out-of-bounds Write	02-Jul-2024	7.8	Improper input validation in copying data to buffer cache in libsaped prior to SMR Jul-2024 Release 1 allows local attackers to write out-of-bounds memory. **CVE ID: CVE-2024-20901**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7232
N/A	02-Jul-2024	7.8	Improper access control in launchApp of SystemUI prior to SMR Jul-2024 Release 1 allows local attackers to launch privileged activities. **CVE ID: CVE-2024-34585**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7233
N/A	02-Jul-2024	7.8	Improper access control in clickAdapterItem of SystemUI prior to SMR Jul-2024 Release 1 allows local attackers to launch privileged activities.	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7234

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-34595		
N/A	02-Jul-2024	6.8	Improper input validation in parsing application information from RTCP packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to execute arbitrary code with system privilege. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34587**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7235
N/A	02-Jul-2024	6.5	Improper input validation?in parsing RTCP SR packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34588**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7236
N/A	02-Jul-2024	6.5	Improper input validation in parsing RTCP RR packet in librtp.so prior to SMR Jul-2024 Release 1	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7237

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34589**		
N/A	02-Jul-2024	5.5	Improper access control in Dar service prior to SMR Jul-2024 Release 1 allows local attackers to bypass restriction for calling SDP features. **CVE ID: CVE-2024-20895**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7238
N/A	02-Jul-2024	5.5	Use of implicit intent for sensitive communication in Configuration message prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information. **CVE ID: CVE-2024-20896**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7239
N/A	02-Jul-2024	5.5	Use of implicit intent for sensitive communication in FCM function in IMS service prior to SMR Jul-2024 Release 1 allows local attackers to	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7240

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 sensitive information. **CVE ID: CVE-2024-20897**		
N/A	02-Jul-2024	5.5	Use of implicit intent for sensitive communication in SoftphoneClient in IMS service prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information. **CVE ID: CVE-2024-20898**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7241
N/A	02-Jul-2024	5.5	Use of implicit intent for sensitive communication in RCS function in IMS service prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information. **CVE ID: CVE-2024-20899**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7242
N/A	02-Jul-2024	5.5	Exposure of sensitive information in proc file system prior to SMR Jul-2024 Release 1 allows local attackers to read kernel memory address. **CVE ID: CVE-2024-34594**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7243
N/A	08-Jul-2024	5.5	Use of implicit intent for sensitive	https://security.samsungmobile	O-SAM-ANDR-250724/7244

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication in Samsung Messages prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34602**	.com/securityUpdate.smsb?year=2024&month=07	
N/A	08-Jul-2024	5.5	Improper access control in Samsung Message prior to SMR Jul-2024 Release 1 allows local attackers to access location data. **CVE ID: CVE-2024-34603**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7245
Improper Authentication	02-Jul-2024	4.3	Improper authentication in BLE prior to SMR Jul-2024 Release 1 allows adjacent attackers to pair with devices. **CVE ID: CVE-2024-20889**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7246
Improper Handling of Exceptional Conditions	02-Jul-2024	4.3	Improper handling of exceptional conditions in Secure Folder prior to SMR Jul-2024 Release 1 allows physical attackers to bypass authentication	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7247

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			under certain condition. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-20894**		
N/A	02-Jul-2024	4.3	Improper input validation in parsing an item type from RTCP SDES packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34590**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7248
N/A	02-Jul-2024	4.3	Improper input validation in parsing an item data from RTCP SDES packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34591**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7249

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Jul-2024	4.3	Improper input validation in parsing RTCP SDES packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34592**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7250
Improper Authentication	02-Jul-2024	3.3	Improper authentication in MTP application prior to SMR Jul-2024 Release 1 allows local attackers to enter MTP mode without proper authentication. **CVE ID: CVE-2024-20900**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7251
N/A	02-Jul-2024	3.3	Improper access control in system property prior to SMR Jul-2024 Release 1 allows local attackers to get device identifier. **CVE ID: CVE-2024-34583**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07	O-SAM-ANDR-250724/7252
N/A	02-Jul-2024	3.3	Improper access control in KnoxCustomManagerService prior to	https://security.samsungmobile.com/securityUpdate.smsb?yea	O-SAM-ANDR-250724/7253

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMR Jul-2024 Release 1 allows local attackers to configure Knox privacy policy. **CVE ID: CVE-2024-34586**	r=2024&month=07	
Product: exynos_1080_firmware					
Affected Version(s): -					
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, and Exynos W930 where they do not properly check length of the data, which can lead to a Denial of Service. **CVE ID: CVE-2024-27360**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27360/	O-SAM-EXYN-250724/7254
Product: exynos_1280_firmware					
Affected Version(s): -					
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, and Exynos W930 where they do not	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/produc	O-SAM-EXYN-250724/7255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			properly check length of the data, which can lead to a Denial of Service. **CVE ID: CVE-2024-27360**	t-security-updates/cve-2024-27360/	
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 1280, Exynos 2200, Exynos 1330, Exynos 1380, and Exynos 2400 where they do not properly check the length of the data, which can lead to a Information disclosure. **CVE ID: CVE-2024-27362**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27362/	O-SAM-EXYN-250724/7256
Product: exynos_1330_firmware					
Affected Version(s): -					
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, and Exynos W930 where they do not properly check length of the data, which can lead to a Denial of Service.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27360/	O-SAM-EXYN-250724/7257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-27360		
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 1280, Exynos 2200, Exynos 1330, Exynos 1380, and Exynos 2400 where they do not properly check the length of the data, which can lead to a Information disclosure. **CVE ID: CVE-2024-27362**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27362/	O-SAM-EXYN-250724/7258
Product: exynos_1380_firmware					
Affected Version(s): -					
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, and Exynos W930 where they do not properly check length of the data, which can lead to a Denial of Service. **CVE ID: CVE-2024-27360**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27360/	O-SAM-EXYN-250724/7259
Improper Validation of Specified	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos	https://semiconductor.samsung.com/support/quality-	O-SAM-EXYN-250724/7260

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Quantity in Input			1280, Exynos 2200, Exynos 1330, Exynos 1380, and Exynos 2400 where they do not properly check the length of the data, which can lead to a Information disclosure. **CVE ID: CVE-2024-27362**	support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27362/	
Product: exynos_2100_firmware					
Affected Version(s): -					
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, and Exynos W930 where they do not properly check length of the data, which can lead to a Denial of Service. **CVE ID: CVE-2024-27360**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27360/	O-SAM-EXYN-250724/7261
Product: exynos_2200_firmware					
Affected Version(s): -					
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/,	O-SAM-EXYN-250724/7262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos 1280, Exynos 1380, Exynos 1330, and Exynos W930 where they do not properly check length of the data, which can lead to a Denial of Service. **CVE ID: CVE-2024-27360**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27360/	
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 1280, Exynos 2200, Exynos 1330, Exynos 1380, and Exynos 2400 where they do not properly check the length of the data, which can lead to a Information disclosure. **CVE ID: CVE-2024-27362**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27362/	O-SAM-EXYN-250724/7263
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 2200 and Exynos 2400 where they lack a check for the validation of native handles, which can result in a DoS(Denial of Service) attack by unmapping an invalid length.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-31957/	O-SAM-EXYN-250724/7264

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-31957		
Product: exynos_2400_firmware					
Affected Version(s): -					
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 1280, Exynos 2200, Exynos 1330, Exynos 1380, and Exynos 2400 where they do not properly check the length of the data, which can lead to a Information disclosure. **CVE ID: CVE-2024-27362**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27362/	O-SAM-EXYN-250724/7265
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 2200 and Exynos 2400 where they lack a check for the validation of native handles, which can result in a DoS(Denial of Service) attack by unmapping an invalid length. **CVE ID: CVE-2024-31957**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-31957/	O-SAM-EXYN-250724/7266
Product: exynos_850_firmware					
Affected Version(s): -					
Improper Validation of Specified	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile	https://semiconductor.samsung.com/support/q	O-SAM-EXYN-250724/7267

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

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Quantity in Input			Processors Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, and Exynos W930 where they do not properly check length of the data, which can lead to a Denial of Service. **CVE ID: CVE-2024-27360**	uality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27360/	
Product: exynos_modem_5300_firmware					
Affected Version(s): -					
N/A	09-Jul-2024	3.7	A vulnerability in Samsung Exynos Modem 5300 allows a Man-in-the-Middle (MITM) attacker to downgrade the security mode of packets going to the victim, enabling the attacker to send messages to the victim in plaintext. **CVE ID: CVE-2024-28067**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-28067/	O-SAM-EXYN-250724/7268
Product: exynos_w930_firmware					
Affected Version(s): -					
Improper Validation of Specified Quantity in Input	09-Jul-2024	7.5	A vulnerability was discovered in Samsung Mobile Processors Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/,	O-SAM-EXYN-250724/7269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos 1280, Exynos 1380, Exynos 1330, and Exynos W930 where they do not properly check length of the data, which can lead to a Denial of Service. **CVE ID: CVE-2024-27360**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27360/	
Vendor: Schneider-electric					
Product: modicon_lmc058_firmware					
Affected Version(s): *					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2024	6.1	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause a vulnerability leading to a cross-site scripting condition where attackers can have a victim's browser run arbitrary JavaScript when they visit a page containing the injected payload. **CVE ID: CVE-2024-6528**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-191-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-191-04.pdf	O-SCH-MODI-250724/7270
Product: modicon_m241_firmware					
Affected Version(s): *					
Improper Neutralization of Input	11-Jul-2024	6.1	CWE-79: Improper Neutralization of Input During Web	https://download.schneider-electric.com/file	O-SCH-MODI-250724/7271

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')			Page Generation ('Cross-site Scripting') vulnerability exists that could cause a vulnerability leading to a cross-site scripting condition where attackers can have a victim's browser run arbitrary JavaScript when they visit a page containing the injected payload. **CVE ID: CVE-2024-6528**	s?p_Doc_Ref=SEVD-2024-191-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-191-04.pdf	
Product: modicon_m251_firmware					
Affected Version(s): *					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2024	6.1	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause a vulnerability leading to a cross-site scripting condition where attackers can have a victim's browser run arbitrary JavaScript when they visit a page containing the injected payload.	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-191-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-191-04.pdf	O-SCH-MODI-250724/7272

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-6528		
Product: modicon_m258_firmware					
Affected Version(s): *					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2024	6.1	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause a vulnerability leading to a cross-site scripting condition where attackers can have a victim's browser run arbitrary JavaScript when they visit a page containing the injected payload. **CVE ID: CVE-2024-6528**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-191-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-191-04.pdf	O-SCH-MODI-250724/7273
Product: modicon_m262_firmware					
Affected Version(s): *					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2024	6.1	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause a vulnerability leading to a cross-site scripting condition where attackers can have	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-191-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-191-04.pdf	O-SCH-MODI-250724/7274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a victim's browser run arbitrary JavaScript when they visit a page containing the injected payload. **CVE ID: CVE-2024-6528**		
Product: whc-5918a_firmware					
Affected Version(s): *					
N/A	11-Jul-2024	7.5	CWE-200: Information Exposure vulnerability exists that could cause disclosure of credentials when a specially crafted message is sent to the device. **CVE ID: CVE-2024-6407**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-191-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-191-01.pdf	O-SCH-WHC--250724/7275
Vendor: supos					
Product: supos					
Affected Version(s): 5.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jul-2024	7.5	supOS 5.0 allows api/image/download?fileName=../ directory traversal for reading files. **CVE ID: CVE-2024-39937**	N/A	O-SUP-SUPO-250724/7276
Vendor: Suse					
Product: linux_enterprise_micro					
Affected Version(s): 6.0					

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
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jul-2024	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE ID: CVE-2024-6387**	https://lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html, https://news.ycombinator.com/item?id=40843778	O-SUS-LINU-250724/7277
Vendor: Tenda					
Product: ac8v4_firmware					
Affected Version(s): 16.03.34.09					
N/A	09-Jul-2024	9.8	Vulnerability in Tenda AC8v4 .V16.03.34.09 due to sscanf and the last digit of s8 being overwritten with \x0. After executing set_client_qos, control over the gp register can be obtained. **CVE ID: CVE-2023-48194**	N/A	O-TEN-AC8V-250724/7278

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

* Stands for all versions