National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
01 – 15 Jul 2023 Vol. 10 No. 13

Table of Content

Vendor	Product	Page Number
Qualcomm	snapdragon_850	902
	snapdragon_855	902
	snapdragon_855\+\/860	904
	snapdragon_865	907
	snapdragon_865\+	907
	snapdragon_865\+_5g	907
	snapdragon_865_5g	910
	snapdragon_870	912
	snapdragon_870_5	913
	snapdragon_870_5g	913
	snapdragon_888	915
	snapdragon_888\+	916
	snapdragon_888\+_5g	916
	snapdragon_888_5g	917
	snapdragon_8\+_gen_1	919
	snapdragon_8_gen_1	921
	snapdragon_ar2_gen_1	924
	snapdragon_auto_4g	925
	snapdragon_auto_5g	926
	snapdragon_w5\+_gen_1	929
	snapdragon_wear_1300	931
	snapdragon_wear_2100	932
	snapdragon_wear_2500	932
	snapdragon_wear_3100	933
	snapdragon_wear_4100\+	934
	snapdragon_x12	935
	snapdragon_x12_lte	936
	snapdragon_x20	936
	snapdragon_x24	937
	snapdragon_x5	938
	snapdragon_x50_5g	938
	snapdragon_x55_5g	940

Vendor	Product	Page Number
Qualcomm	ipq8071a_firmware	1473
	ipq8072a_firmware	1474
	ipq8074a_firmware	1475
	ipq8076a_firmware	1476
	ipq8076_firmware	1477
	ipq8078a_firmware	1478
	ipq8078_firmware	1479
	ipq8173_firmware	1479
	ipq8174_firmware	1480
	ipq9008_firmware	1481
	ipq9574_firmware	1482
	mdm9250_firmware	1483
	mdm9628_firmware	1483
	mdm9640_firmware	1484
	mdm9650_firmware	1484
	msm8108_firmware	1485
	msm8209_firmware	1486
	msm8608_firmware	1487
	msm8909w_firmware	1487
	msm8996au_firmware	1488
	pmp8074_firmware	1489
	qam8255p_firmware	1489
	qam8295p_firmware	1491
	qam8650p_firmware	1493
	qam8775p_firmware	1494
	qca4004_firmware	1495
	qca4024_firmware	1495
	qca6174a_firmware	1496
	qca6175a_firmware	1498
	qca6310_firmware	1498
	qca6320_firmware	1500
	qca6335_firmware	1502

Vendor	Product	Page Number
Qualcomm	qca9377_firmware	1555
	qca9379_firmware	1557
	qca9880_firmware	1557
	qca9886_firmware	1558
	qca9888_firmware	1558
	qca9889_firmware	1559
	qca9898_firmware	1560
	qca9980_firmware	1560
	qca9984_firmware	1561
	qca9985_firmware	1561
	qca9986_firmware	1561
	qca9990_firmware	1562
	qca9992_firmware	1562
	qca9994_firmware	1563
	qcm2290_firmware	1563
	qcm4290_firmware	1565
	qcm4325_firmware	1566
	qcm4490_firmware	1568
	qcm6125_firmware	1569
	qcm6490_firmware	1570
	qcn5021_firmware	1572
	qcn5022_firmware	1572
	qcn5024_firmware	1573
	qcn5052_firmware	1574
	qcn5054_firmware	1575
	qcn5122_firmware	1576
	qcn5124_firmware	1577
	qcn5152_firmware	1578
	qcn5154_firmware	1579
	qcn5164_firmware	1580
	qcn6023_firmware	1581
	qcn6024_firmware	1582

Vendor	Product	Page Number
Qualcomm	qcn6100_firmware	1583
	qcn6102_firmware	1584
	qcn6112_firmware	1584
	qcn6122_firmware	1584
	qcn6132_firmware	1585
	qcn7605_firmware	1586
	qcn7606_firmware	1586
	qcn9000_firmware	1586
	qcn9001_firmware	1587
	qcn9002_firmware	1588
	qcn9003_firmware	1589
	qcn9011_firmware	1590
	qcn9012_firmware	1591
	qcn9022_firmware	1593
	qcn9024_firmware	1593
	qcn9070_firmware	1595
	qcn9072_firmware	1596
	qcn9074_firmware	1597
	qcn9100_firmware	1598
	qcn9274_firmware	1599
	qcs2290_firmware	1600
	qcs410_firmware	1601
	qcs4290_firmware	1603
	qcs4490_firmware	1604
	qcs610_firmware	1606
	qcs6125_firmware	1608
	qcs6490_firmware	1609
	qcs8155_firmware	1610
	qcs8250_firmware	1611
	qcs8550_firmware	1612
	qrb5165m_firmware	1612
	qrb5165n_firmware	1614

Vendor	Product	Page Number
Qualcomm	qsm8250_firmware	1615
	qsm8350_firmware	1616
	qts110_firmware	1616
	robotics_rb3_firmware	1616
	robotics_rb5_firmware	1617
	sa4150p_firmware	1619
	sa4155p_firmware	1621
	sa6145p_firmware	1622
	sa6150p_firmware	1625
	sa6155p_firmware	1628
	sa6155_firmware	1632
	sa8145p_firmware	1633
	sa8150p_firmware	1636
	sa8155p_firmware	1639
	sa8155_firmware	1642
	sa8195p_firmware	1643
	sa8255p_firmware	1646
	sa8295p_firmware	1648
	sc8180x-aaab_firmware	1650
	sc8180x-aa_firmware	1650
	sc8180x-ab_firmware	1651
	sc8180x-acaf_firmware	1651
	sc8180x-ac_firmware	1651
	sc8180x-ad_firmware	1651
	sc8180x-af_firmware	1652
	sc8180xp-aaab_firmware	1652
	sc8180xp-aa_firmware	1653
	sc8180xp-ab_firmware	1653
	sc8180xp-acaf_firmware	1653
	sc8180xp-ac_firmware	1653
	sc8180xp-ad_firmware	1654
	sc8180xp-af_firmware	1654

Vendor	Product	Page Number
Qualcomm	sc8180x\+sdx55_firmware	1655
	sd460_firmware	1655
	sd626_firmware	1655
	sd660_firmware	1656
	sd662_firmware	1658
	sd670_firmware	1658
	sd675_firmware	1659
	sd730_firmware	1660
	sd820_firmware	1661
	sd821_firmware	1662
	sd835_firmware	1662
	sd855_firmware	1664
	sd865_5g_firmware	1666
	sd888_firmware	1669
	sdm429w_firmware	1671
	sdx20m_firmware	1672
	sdx55_firmware	1672
	sdx57m_firmware	1674
	sdx65m_firmware	1674
	sd_455_firmware	1675
	sd_675_firmware	1676
	sd_8_gen1_5g_firmware	1677
	sg4150p_firmware	1678
	sm4125_firmware	1680
	sm6250p_firmware	1681
	sm6250_firmware	1682
	sm7250p_firmware	1683
	sm7315_firmware	1684
	sm7325p_firmware	1686
	smart_audio_200_firmware	1688
	smart_audio_400_firmware	1689
	smart_display_200_firmware	1691

Vendor	Product	Page Number
Qualcomm	snapdragon_208_firmware	1692
	snapdragon_210_firmware	1692
	snapdragon_212_firmware	1693
	snapdragon_425_firmware	1694
	snapdragon_427_firmware	1695
	snapdragon_429_firmware	1695
	snapdragon_430_firmware	1696
	snapdragon_435_firmware	1697
	snapdragon_439_firmware	1697
	snapdragon_450_firmware	1699
	snapdragon_460_firmware	1699
	snapdragon_480\+_5g_firmware	1701
	snapdragon_480_5g_firmware	1702
	snapdragon_4_gen_1_firmware	1704
	snapdragon_4_gen_2_firmware	1706
	snapdragon_625_firmware	1708
	snapdragon_626_firmware	1708
	snapdragon_630_firmware	1709
	snapdragon_632_firmware	1710
	snapdragon_636_firmware	1710
	snapdragon_660_firmware	1711
	snapdragon_662_firmware	1713
	snapdragon_665_firmware	1715
	snapdragon_670_firmware	1716
	snapdragon_675_firmware	1717
	snapdragon_678_firmware	1718
	snapdragon_680_4g_firmware	1719
	snapdragon_685_4g_firmware	1721
	snapdragon_690_5g_firmware	1723
	snapdragon_695_5g_firmware	1725
	snapdragon_710_firmware	1726
	snapdragon_712_firmware	1727

Vendor	Product	Page Number
Qualcomm	snapdragon_720g_firmware	1728
	snapdragon_730g_firmware	1729
	snapdragon_730_firmware	1730
	snapdragon_732g_firmware	1731
	snapdragon_750g_5g_firmware	1732
	snapdragon_765g_5g_firmware	1734
	snapdragon_765_5g_firmware	1736
	snapdragon_768g_5g_firmware	1737
	snapdragon_778g\+_5g_firmware	1739
	snapdragon_778g\+_firmware	1741
	snapdragon_778g_5g_firmware	1741
	snapdragon_780g_5g_firmware	1743
	snapdragon_780g_firmware	1745
	snapdragon_782g_firmware	1745
	snapdragon_7c\+_gen_3_firmware	1747
	snapdragon_7c_firmware	1749
	snapdragon_7c_gen_2_firmware	1749
	snapdragon_820_firmware	1749
	snapdragon_821_firmware	1750
	snapdragon_835_firmware	1750
	snapdragon_845_firmware	1752
	snapdragon_850_firmware	1753
	snapdragon_855\+\/860_firmware	1753
	snapdragon_855_firmware	1755
	snapdragon_865\+_5g_firmware	1758
	snapdragon_865\+_firmware	1760
	snapdragon_865_5g_firmware	1761
	snapdragon_865_firmware	1763
	snapdragon_870_5g_firmware	1764
	snapdragon_870_5_firmware	1766
	snapdragon_870_firmware	1766
	snapdragon_888\+_5g_firmware	1767

Vendor	Product	Page Number
Qualcomm	snapdragon_888\+_firmware	1768
	snapdragon_888_5g_firmware	1769
	snapdragon_888_firmware	1770
	snapdragon_8\+_gen_1_firmware	1770
	snapdragon_8_gen_1_firmware	1772
	snapdragon_ar2_gen_1_firmware	1775
	snapdragon_auto_4g_firmware	1776
	snapdragon_auto_5g_firmware	1778
	snapdragon_w5\+_gen_1_firmware	1780
	snapdragon_wear_1300_firmware	1783
	snapdragon_wear_2100_firmware	1783
	snapdragon_wear_2500_firmware	1784
	snapdragon_wear_3100_firmware	1785
	snapdragon_wear_4100\+_firmware	1785
	snapdragon_x12_firmware	1786
	snapdragon_x12_lte_firmware	1787
	snapdragon_x20_firmware	1788
	snapdragon_x24_firmware	1788
	snapdragon_x50_5g_firmware	1789
	snapdragon_x55_5g_firmware	1791
	snapdragon_x5_firmware	1794
	snapdragon_x65_5g_firmware	1794
	snapdragon_x70_firmware	1796
	snapdragon_xr1_firmware	1796
	snapdragon_xr2\+_gen_1_firmware	1797
	snapdragon_xr2_5g_firmware	1798
	ssg2115p_firmware	1801
	ssg2125p_firmware	1802
	sw5100p_firmware	1803
	sw5100_firmware	1806
	sxr1120_firmware	1809
	sxr1230p_firmware	1810

Vendor	Product	Page Number
Qualcomm	sxr2130_firmware	1811
	sxr2230p_firmware	1814
	video_collaboration_vc1_firmware	1815
	video_collaboration_vc3_firmware	1817
	video_collaboration_vc5_firmware	1819
	vision_intelligence_100_firmware	1820
	vision_intelligence_200_firmware	1820
	vision_intelligence_300_firmware	1821
	vision_intelligence_400_firmware	1821
	wcd9306_firmware	1822
	wcd9326_firmware	1822
	wcd9335_firmware	1824
	wcd9340_firmware	1827
	wcd9341_firmware	1829
	wcd9360_firmware	1832
	wcd9370_firmware	1833
	wcd9371_firmware	1836
	wcd9375_firmware	1837
	wcd9380_firmware	1839
	wcd9385_firmware	1843
	wcn3610_firmware	1845
	wcn3615_firmware	1847
	wcn3620_firmware	1848
	wcn3660b_firmware	1850
	wcn3660_firmware	1852
	wcn3680b_firmware	1852
	wcn3680_firmware	1855
	wcn3910_firmware	1855
	wcn3950_firmware	1857
	wcn3980_firmware	1859
	wcn3988_firmware	1862
	wcn3990_firmware	1865

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 2fauth					
Product: 2fauth					
Affected Version(s): * Up to (excluding) 4.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jul-2023	6.1	2FA is a Web app to manage Two-Factor Authentication (2FA) accounts and generate their security codes. Cross site scripting (XSS) injection can be done via the account/service field. This was tested in docker-compose environment. This vulnerability has been patched in version 4.0.3. **CVE ID : CVE-2023-36816**	https://github.com/Bubka/2FAuth/security/advisories/GHSA-cwhq-2mcq-pp9q	A-2FA-2FAU-240723/1
Vendor: activeitzone					
Product: active_ecommerce_cms					
Affected Version(s): 6.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jul-2023	6.1	A vulnerability was found in Active It Zone Active eCommerce CMS 6.5.0. It has been declared as problematic. This vulnerability affects unknown code of the file /ecommerce/support_ticket of the component Create	N/A	A-ACT-ACTI-240723/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ticket Page. The manipulation of the argument details with the input <script>alert(1)</script> leads to cross site scripting. The attack can be initiated remotely. VDB-232954 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3506**		
Vendor: anydesk					
Product: anydesk					
Affected Version(s): 7.0.8					
Uncontrolled Resource Consumption	03-Jul-2023	7.5	AnyDesk 7.0.8 allows remote Denial of Service. **CVE ID : CVE-2023-26509**	N/A	A-ANY-ANYD-240723/3
Vendor: an_gradebook_project					
Product: an_gradebook					
Affected Version(s): * Up to (including) 5.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	4.8	The AN_GradeBook WordPress plugin through 5.0.1 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	N/A	A-AN_-AN_G-240723/4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID : CVE-2023-2709**		
Vendor: Apache					
Product: any23					
Affected Version(s): * Up to (including) 2.7					
Improper Input Validation	05-Jul-2023	5.3	** UNSUPPPORTED WHEN ASSIGNED ** ** UNSUPPORTED WHEN ASSIGNED ** Use of TikaEncodingDetector in Apache Any23 can cause excessive memory usage. **CVE ID : CVE-2023-34150**	https://lists.apache.org/thread/713tk23khbtbg940pb2ql8ggd4cvh6j1	A-APA-ANY2-240723/5
Product: apache-airflow-providers-apache-hive					
Affected Version(s): * Up to (excluding) 6.1.1					
Improper Input Validation	03-Jul-2023	9.8	Improper Input Validation vulnerability in Apache Software Foundation Apache Airflow Hive Provider. This issue affects Apache Airflow Apache Hive Provider: before 6.1.1. Before version 6.1.1 it was possible to bypass the security check to RCE via	https://github.com/apache/airflow/pull/31983, https://lists.apache.org/thread/30y19ok07fw52x5hnkbhwqo3ho0wwc1y	A-APA-APAC-240723/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			principal parameter. For this to be exploited it requires access to modifying the connection details. It is recommended updating provider version to 6.1.1 in order to avoid this vulnerability. **CVE ID : CVE-2023-35797**		
Product: johnzon					
Affected Version(s): * Up to (excluding) 1.2.21					
Deserialization of Untrusted Data	07-Jul-2023	5.3	Deserialization of Untrusted Data vulnerability in Apache Software Foundation Apache Johnzon. A malicious attacker can craft up some JSON input that uses large numbers (numbers such as 1e20000000) that Apache Johnzon will deserialize into BigDecimal and maybe use numbers too large which may result in a slow conversion (Denial of service risk). Apache	https://lists.apache.org/thread/qbg14djo95gfpk7o560lr8wcrzfyw43l	A-APA-JOHN-240723/7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Johnzon 1.2.21 mitigates this by setting a scale limit of 1000 (by default) to the BigDecimal. This issue affects Apache Johnzon: through 1.2.20. **CVE ID : CVE-2023-33008**		
Vendor: Arcserve					
Product: udp					
Affected Version(s): * Up to (including) 9.0.6034					
Incorrect Authorization	03-Jul-2023	9.8	Arcserve UDP through 9.0.6034 allows authentication bypass. The method getVersionInfo at WebServiceImpl/services/FlashServiceImpl leaks the AuthUUID token. This token can be used at /WebServiceImpl/services/VirtualStandbyServiceImpl to obtain a valid session. This session can be used to execute any task as administrator. **CVE ID : CVE-2023-26258**	N/A	A-ARC-UDP-240723/8
Vendor: Arubanetworks					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mc-va-10					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jul-2023	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-35975**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/9
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jul-2023	7.5	There is an unauthenticated buffer overflow vulnerability in the process controlling the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in a Denial-of-Service (DoS) condition affecting the web-based management interface of the controller. **CVE ID : CVE-2023-35979**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/10
Improper Neutralization of Special Elements used in a Command	05-Jul-2023	7.2	An authenticated remote command injection vulnerability exists in the ArubaOS web-based management interface. Successful	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/11

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-35972**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35973**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/12
Improper Neutralization of Special Elements used in a Command ('Comman	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35974**		
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35976**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/14
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35977**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/15

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in the ArubaOS web-based management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35971**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/16
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in ArubaOS could allow an unauthenticated remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based management interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35978**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/17
Product: mc-va-1k					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jul-2023	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-35975**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/18
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jul-2023	7.5	There is an unauthenticated buffer overflow vulnerability in the process controlling the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in a Denial-of-Service (DoS) condition affecting the web-based management interface of the controller. **CVE ID : CVE-2023-35979**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/19
Improper Neutralization of Special Elements used in a Command ('Comman	05-Jul-2023	7.2	An authenticated remote command injection vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/20

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-35972**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35973**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/21
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/22

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user on the underlying operating system. **CVE ID : CVE-2023-35974**		
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35976**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/23
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35977**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/24
Improper Neutralizat	05-Jul-2023	6.1	A vulnerability in the ArubaOS web-based	https://www.arubanetw	A-ARU-MC-V-240723/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35971**	orks.com/assets/alert/ARUBA-PSA-2023-008.txt	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in ArubaOS could allow an unauthenticated remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based management interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35978**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/26
Product: mc-va-250					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jul-2023	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-35975**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/27
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jul-2023	7.5	There is an unauthenticated buffer overflow vulnerability in the process controlling the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in a Denial-of-Service (DoS) condition affecting the web-based management interface of the controller. **CVE ID : CVE-2023-35979**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/28
Improper Neutralization of Special Elements used in a Command ('Comman	05-Jul-2023	7.2	An authenticated remote command injection vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/29

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-35972**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35973**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/30
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/31

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system. **CVE ID : CVE-2023-35974**		
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35976**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/32
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35977**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/33
Improper Neutralization of Input	05-Jul-2023	6.1	A vulnerability in the ArubaOS web-based management interface could allow	https://www.arubanetworks.com/assets/alert/A	A-ARU-MC-V-240723/34

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35971**	RUBA-PSA-2023-008.txt	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in ArubaOS could allow an unauthenticated remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based management interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35978**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/35
Product: mc-va-50					
Affected Version(s): -					
Improper Limitation of a	05-Jul-2023	8.1	An authenticated path traversal vulnerability exists	https://www.arubanetworks.com/as	A-ARU-MC-V-240723/36

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-35975**	sets/alert/ARUBA-PSA-2023-008.txt	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jul-2023	7.5	There is an unauthenticated buffer overflow vulnerability in the process controlling the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in a Denial-of-Service (DoS) condition affecting the web-based management interface of the controller. **CVE ID : CVE-2023-35979**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/37
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	An authenticated remote command injection vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/38

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-35972**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35973**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/39
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/40

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35974		
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35976**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/41
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35977**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/42
Improper Neutralization of Input During Web Page	05-Jul-2023	6.1	A vulnerability in the ArubaOS web-based management interface could allow an unauthenticated remote attacker	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35971**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in ArubaOS could allow an unauthenticated remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based management interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35978**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MC-V-240723/44
Product: mcr-va-10k					
Affected Version(s): -					
Improper Limitation of a Pathname to a	05-Jul-2023	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line	https://www.arubanetworks.com/assets/alert/A	A-ARU-MCR--240723/45

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-35975**	RUBA-PSA-2023-008.txt	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jul-2023	7.5	There is an unauthenticated buffer overflow vulnerability in the process controlling the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in a Denial-of-Service (DoS) condition affecting the web-based management interface of the controller. **CVE ID : CVE-2023-35979**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/46
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	An authenticated remote command injection vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/47

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-35972**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35973**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/48
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35974**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/49

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35976**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/50
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35977**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/51
Improper Neutralization of Input During Web Page Generation	05-Jul-2023	6.1	A vulnerability in the ArubaOS web-based management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35971**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in ArubaOS could allow an unauthenticated rem ote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based management interfac e. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35978**	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-008.txt	A-ARU-MCR--240723/53
Product: mcr-va-1k					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory	05-Jul-2023	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-008.txt	A-ARU-MCR--240723/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-35975**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jul-2023	7.5	There is an unauthenticated buffer overflow vulnerability in the process controlling the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in a Denial-of-Service (DoS) condition affecting the web-based management interface of the controller. **CVE ID : CVE-2023-35979**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/55
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	An authenticated remote command injection vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/56

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-35972**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35973**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/57
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35974**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/58
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated	https://www.arubanetworks.com/as	A-ARU-MCR--240723/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35976**	sets/alert/ARUBA-PSA-2023-008.txt	
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35977**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/60
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in the ArubaOS web-based management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/61

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35971**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in ArubaOS could allow an unauthenticated remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based management interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35978**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/62
Product: mcr-va-50					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jul-2023	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/63

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the underlying operating system. **CVE ID : CVE-2023-35975**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jul-2023	7.5	There is an unauthenticated buffer overflow vulnerability in the process controlling the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in a Denial-of-Service (DoS) condition affecting the web-based management interface of the controller. **CVE ID : CVE-2023-35979**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/64
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	An authenticated remote command injection vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/65

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system on the device running ArubaOS. **CVE ID : CVE-2023-35972**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35973**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/66
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35974**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/67
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access	https://www.arubanetworks.com/assets/alert/A	A-ARU-MCR--240723/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35976**	RUBA-PSA-2023-008.txt	
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35977**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/69
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in the ArubaOS web-based management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35971**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in ArubaOS could allow an unauthenticated remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based management interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35978**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/71
Product: mcr-va-500					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jul-2023	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35975		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jul-2023	7.5	There is an unauthenticated buffer overflow vulnerability in the process controlling the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in a Denial-of-Service (DoS) condition affecting the web-based management interface of the controller. **CVE ID : CVE-2023-35979**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/73
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	An authenticated remote command injection vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/74

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35972		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35973**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/75
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35974**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/76
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/77

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35976**		
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35977**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/78
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in the ArubaOS web-based management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/79

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35971**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in ArubaOS could allow an unauthenticated remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based management interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35978**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/80
Product: mcr-va-5k					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jul-2023	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/81

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35975		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jul-2023	7.5	There is an unauthenticated buffer overflow vulnerability in the process controlling the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in a Denial-of-Service (DoS) condition affecting the web-based management interface of the controller. **CVE ID : CVE-2023-35979**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/82
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	An authenticated remote command injection vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/83

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35972		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35973**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/84
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35974**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/85
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35976**		
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35977**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/87
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in the ArubaOS web-based management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35971**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in ArubaOS could allow an unauthenticated remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based management interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35978**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-MCR--240723/89
Product: sd-wan					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jul-2023	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-SD-W-240723/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35975		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jul-2023	7.5	There is an unauthenticated buffer overflow vulnerability in the process controlling the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in a Denial-of-Service (DoS) condition affecting the web-based management interface of the controller. **CVE ID : CVE-2023-35979**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-SD-W-240723/91
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	An authenticated remote command injection vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-SD-W-240723/92

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35972		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35973**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-SD-W-240723/93
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35974**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-SD-W-240723/94
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-SD-W-240723/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35976**		
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35977**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-SD-W-240723/96
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in the ArubaOS web-based management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-SD-W-240723/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35971**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in ArubaOS could allow an unauthenticated remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based management interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35978**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	A-ARU-SD-W-240723/98
Vendor: bagesoft					
Product: bagecms					
Affected Version(s): 3.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2023	5.4	A stored cross-site scripting (XSS) vulnerability in Bagecms v3.1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Custom Settings module.	N/A	A-BAG-BAGE-240723/99

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37122		
Vendor: bbs-go					
Product: bbs-go					
Affected Version(s): * Up to (including) 3.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jul-2023	5.4	Cross Site Scripting vulnerability in mlogclub bbs-go v. 3.5.5. and before allows a remote attacker to execute arbitrary code via a crafted payload to the comment parameter in the article function. **CVE ID : CVE-2023-36222**	N/A	A-BBS-BBS--240723/100
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jul-2023	5.4	Cross Site Scripting vulnerability in mlogclub bbs-go v. 3.5.5. and before allows a remote attacker to execute arbitrary code via a crafted payload to the announcements parameter in the settings function. **CVE ID : CVE-2023-36223**	N/A	A-BBS-BBS--240723/101
Vendor: bigcontact_contact_page_project					
Product: bigcontact_contact_page					
Affected Version(s): * Up to (including) 1.5.8					
Cross-Site Request Forgery (CSRF)	10-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Arian Khosravi, Norik Davtian BigContact	N/A	A-BIG-BIGC-240723/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Contact Page plugin <= 1.5.8 versions. **CVE ID : CVE-2023-22694**		
Vendor: Bouncycastle					
Product: bc-java					
Affected Version(s): * Up to (excluding) 1.74					
Improper Certificate Validation	05-Jul-2023	5.3	Bouncy Castle For Java before 1.74 is affected by an LDAP injection vulnerability. The vulnerability only affects applications that use an LDAP CertStore from Bouncy Castle to validate X.509 certificates. During the certificate validation process, Bouncy Castle inserts the certificate's Subject Name into an LDAP search filter without any escaping, which leads to an LDAP injection vulnerability. **CVE ID : CVE-2023-33201**	https://github.com/bcgit/bc-java/commit/e8c409a8389c815ea3fda5e8b94c92fdfe583bcc, https://github.com/bcgit/bc-java/wiki/CVE-2023-33201	A-BOU-BC-J-240723/103
Vendor: Brave					
Product: browser					
Affected Version(s): * Up to (excluding) 1.52.117					
URL Redirection to Untrusted	01-Jul-2023	6.1	An Open Redirect vulnerability exists prior to version 1.52.117, where the built-in QR scanner in Brave Browser	N/A	A-BRA-BROW-240723/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Site ('Open Redirect')			Android navigated to scanned URLs automatically without showing the URL first. Now the user must manually navigate to the URL. **CVE ID : CVE-2023-28364**		
Vendor: Chamilo					
Product: chamilo					
Affected Version(s): From (including) 1.11.0 Up to (including) 1.11.20					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	4.8	Chamilo 1.11.x up to 1.11.20 allows users with an admin privilege account to insert XSS in the languages management section. **CVE ID : CVE-2023-37061**	https://github.com/chamilo/chamilo-lms/commit/75e9b3e0acac6f7a643da6ff19a00d55a94417a1, https://support.chamilo.org/projects/1/wiki/Security_issues#Issue-116-2023-06-06-Low-impact-Low-risk-XSS-through-admin-account-languages-management	A-CHA-CHAM-240723/105
Improper Neutralization of Input During Web Page Generation	07-Jul-2023	4.8	Chamilo 1.11.x up to 1.11.20 allows users with admin privilege account to insert XSS in the course categories' definition.	https://github.com/chamilo/chamilo-lms/commit/c263933d1d958edee3999820f636c8cb919d03d	A-CHA-CHAM-240723/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-37062**	1, https://support.chamilo.org/projects/1/wiki/Security_issues#Issue-115-2023-06-06-Low-impact-Low-risk-XSS-through-admin-account-course-category	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	4.8	Chamilo 1.11.x up to 1.11.20 allows users with admin privilege account to insert XSS in the careers & promotions management section. **CVE ID : CVE-2023-37063**	https://support.chamilo.org/projects/1/wiki/Security_issues#Issue-117-2023-06-06-Low-impact-Low-risk-XSS-through-admin-account-careers-amp-promotions-management, https://github.com/chamilo/chamilo-lms/commit/546a18b0bd1446123f4e29f81f42e71b761f51b7	A-CHA-CHAM-240723/107
Improper Neutralization of	07-Jul-2023	4.8	Chamilo 1.11.x up to 1.11.20 allows users with admin privilege	https://support.chamilo.org/projects/	A-CHA-CHAM-240723/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			account to insert XSS in the extra fields management section. **CVE ID : CVE-2023-37064**	1/wiki/Security_issues#Issue-119-2023-06-06-Low-impact-Low-risk-XSS-through-admin-account-extra-fields-management, https://github.com/chamilo/chamilo-lms/commit/91ecc6141de6de9483c5a31fbb9fa91450f24940	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	4.8	Chamilo 1.11.x up to 1.11.20 allows users with admin privilege account to insert XSS in the session category management section. **CVE ID : CVE-2023-37065**	https://support.chamilo.org/projects/1/wiki/Security_issues#Issue-118-2023-06-06-Low-impact-Low-risk-XSS-through-admin-account-session-category-management, https://github.com/chamilo/chamilo-lms/commit/da61f287d2e508a5e94	A-CHA-CHAM-240723/109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				0953b474051d0f21e91c0	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	4.8	Chamilo 1.11.x up to 1.11.20 allows users with admin privilege account to insert XSS in the skills wheel. **CVE ID : CVE-2023-37066**	https://support.chamilo.org/projects/1/wiki/Security_issues#Issue-114-2023-06-06-Low-impact-Low-risk-XSS-through-admin-account-skills, https://github.com/chamilo/chamilo-lms/commit/4f7b5ebf90c35999917c231276e47a4184275690	A-CHA-CHAM-240723/110
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	4.8	Chamilo 1.11.x up to 1.11.20 allows users with admin privilege account to insert XSS in the classes/usergroups management section. **CVE ID : CVE-2023-37067**	https://support.chamilo.org/projects/1/wiki/Security_issues#Issue-120-2023-06-07-Low-impact-Low-risk-XSS-through-admin-account-classesusergroups-management, https://github.com/chamilo/chamilo-lms/commit	A-CHA-CHAM-240723/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				/c75ff227bcf00e9f88e9477b78eaeed9e0668905	
Vendor: chatengine_project					
Product: chatengine					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2023	9.6	Cross Site Scripting (XSS) vulnerability in username field in /src/chatbotapp/LoginServlet.java in wliang6 ChatEngine commit fded8e710ad59f816867ad47d7fc4862f6502f3e, allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30319**	https://payatu.com/advisory/cross-site-scripting-xxs-vulnerability-in-wliang6-chatengine/	A-CHA-CHAT-240723/112
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2023	9	Cross Site Scripting (XSS) vulnerability in textMessage field in /src/chatbotapp/chatWindow.java in wliang6 ChatEngine commit fded8e710ad59f816867ad47d7fc4862f6502f3e, allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30320**	https://payatu.com/advisory/cross-site-scripting-xss-vulnerability-in-wliang6-chatengine-allows-attackers-execute-arbitrary-code/	A-CHA-CHAT-240723/113
Improper Neutralization of Input During Web Page	06-Jul-2023	9	Cross Site Scripting (XSS) vulnerability in textMessage field in /src/chatbotapp/LoginServlet.java in wliang6 ChatEngine	https://payatu.com/advisory/cross-site-scripting-xss-	A-CHA-CHAT-240723/114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			commit fded8e710ad59f816867ad47d7fc4862f6502f3e, allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30321**	vulnerability-in-loginservlet-java-wliang6-chatengine-allows-attackers-to-execute-arbitrary-code/	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jul-2023	7.5	SQL Injection vulnerability in username field in /src/chatbotapp/chatWindow.java in Payatu ChatEngine v.1.0, allows attackers to gain sensitive information. **CVE ID : CVE-2023-30323**	https://payatu.com/advisory/sql-injection-in-chatwindow-functionality-in-chatengine-1-0/	A-CHA-CHAT-240723/115
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jul-2023	7.5	SQL Injection vulnerability in textMessage parameter in /src/chatbotapp/chatWindow.java in wliang6 ChatEngine v.1.0, allows attackers to gain sensitive information. **CVE ID : CVE-2023-30325**	https://payatu.com/advisory/sql-injection-vulnerability-in-textmessage-field-in-chatengine-1-0/	A-CHA-CHAT-240723/116
Improper Neutralization of Input During Web Page	06-Jul-2023	6.1	Cross Site Scripting (XSS) vulnerability in username field in /WebContent/WEB-INF/lib/chatbox.jsp in wliang6	https://payatu.com/advisory/cross-site-scripting-vulnerability	A-CHA-CHAT-240723/117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			ChatEngine commit fded8e710ad59f816867ad47d7fc4862f6502f3e, allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30326**	-in-username-field-in-chatbox-functionality-in-chatengine-1-0/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2023	5.4	Cross Site Scripting (XSS) vulnerability in username field in /src/chatbotapp/chatWindow.java in Payatu ChatEngine v.1.0, allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30322**	https://payatu.com/advisory/cross-site-scripting-xss-in-username-field-in-chatwindow-functionality-in-chatengine-1-0/	A-CHA-CHAT-240723/118
Vendor: Citrix					
Product: application_delivery_controller					
Affected Version(s): From (including) 12.1 Up to (excluding) 12.1-55.296					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	6.1	Cross site scripting vulnerability in Citrix ADC and Citrix Gateway? in allows and attacker to perform cross site scripting **CVE ID : CVE-2023-24488**	https://support.citrix.com/article/CTX477714/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202324487-cve202324488	A-CIT-APPL-240723/119
Affected Version(s): From (including) 12.1 Up to (excluding) 12.1-65.35					
Improper Neutralization of	10-Jul-2023	6.1	Cross site scripting vulnerability in Citrix ADC and Citrix	https://support.citrix.com/article/C	A-CIT-APPL-240723/120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Gateway? in allows and attacker to perform cross site scripting **CVE ID : CVE-2023-24488**	TX477714/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202324487-cve202324488	
Affected Version(s): From (including) 13.0 Up to (excluding) 13.0-90.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	6.1	Cross site scripting vulnerability in Citrix ADC and Citrix Gateway? in allows and attacker to perform cross site scripting **CVE ID : CVE-2023-24488**	https://support.citrix.com/article/CTX477714/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202324487-cve202324488	A-CIT-APPL-240723/121
Affected Version(s): From (including) 13.1 Up to (excluding) 13.1-45.61					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	6.1	Cross site scripting vulnerability in Citrix ADC and Citrix Gateway? in allows and attacker to perform cross site scripting **CVE ID : CVE-2023-24488**	https://support.citrix.com/article/CTX477714/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202324487-cve202324488	A-CIT-APPL-240723/122
Product: gateway					
Affected Version(s): From (including) 12.1 Up to (excluding) 12.1-65.35					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	6.1	Cross site scripting vulnerability in Citrix ADC and Citrix Gateway? in allows and attacker to perform cross site scripting **CVE ID : CVE-2023-24488**	https://support.citrix.com/article/CTX477714/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202324487-cve202324488	A-CIT-GATE-240723/123
Affected Version(s): From (including) 13.0 Up to (excluding) 13.0-90.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	6.1	Cross site scripting vulnerability in Citrix ADC and Citrix Gateway? in allows and attacker to perform cross site scripting **CVE ID : CVE-2023-24488**	https://support.citrix.com/article/CTX477714/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202324487-cve202324488	A-CIT-GATE-240723/124
Affected Version(s): From (including) 13.1 Up to (excluding) 13.1-45.61					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	6.1	Cross site scripting vulnerability in Citrix ADC and Citrix Gateway? in allows and attacker to perform cross site scripting **CVE ID : CVE-2023-24488**	https://support.citrix.com/article/CTX477714/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202324487-cve202324488	A-CIT-GATE-240723/125
Vendor: Cmsmadesimple					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: cms_made_simple					
Affected Version(s): 2.2.17					
Unrestricted Upload of File with Dangerous Type	06-Jul-2023	8.8	CMS Made Simple v2.2.17 is vulnerable to Remote Command Execution via the File Upload Function. **CVE ID : CVE-2023-36969**	N/A	A-CMS-CMS_-240723/126
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2023	5.4	A Cross-site scripting (XSS) vulnerability in CMS Made Simple v2.2.17 allows remote attackers to inject arbitrary web script or HTML via the File Upload function. **CVE ID : CVE-2023-36970**	N/A	A-CMS-CMS_-240723/127
Vendor: codeermeneer					
Product: companion_sitemap_generator					
Affected Version(s): * Up to (excluding) 4.5.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	6.1	The Companion Sitemap Generator WordPress plugin before 4.5.3 does not sanitise and escape some parameters before outputting them back in pages, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin. **CVE ID : CVE-2023-1780**	N/A	A-COD-COMP-240723/128
Vendor: comment_reply_notification_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: comment_reply_notification					
Affected Version(s): * Up to (including) 1.4					
Cross-Site Request Forgery (CSRF)	11-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Denishua Comment Reply Notification plugin <= 1.4 versions. **CVE ID : CVE-2023-25051**	N/A	A-COM-COMM-240723/129
Vendor: configurable_tag_cloud_project					
Product: configurable_tag_cloud					
Affected Version(s): * Up to (excluding) 5.3					
Cross-Site Request Forgery (CSRF)	10-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Keith Solomon Configurable Tag Cloud (CTC) plugin <= 5.2 versions. **CVE ID : CVE-2023-28995**	N/A	A-CON-CONF-240723/130
Vendor: darktrace					
Product: threat_visualizer					
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.0.15					
Incorrect Authorization	06-Jul-2023	6.1	An improper authorization vulnerability in Darktrace mobile app (Android) prior to version 6.0.15 allows disabled and low-privilege users to control "antigena" actions(block/unblock traffic) from the mobile application. This vulnerability could create a	N/A	A-DAR-THRE-240723/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			"shutdown", blocking all ingress or egress traffic in the entire infrastructure where darktrace agents are deployed. **CVE ID : CVE-2023-29656**		
Vendor: database_collation_fix_project					
Product: database_collation_fix					
Affected Version(s): * Up to (excluding) 1.2.8					
Cross-Site Request Forgery (CSRF)	11-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Dave Jesch Database Collation Fix plugin <= 1.2.7 versions. **CVE ID : CVE-2023-23997**	N/A	A-DAT-DATA-240723/132
Vendor: diagon_project					
Product: diagon					
Affected Version(s): 1.0.139					
Out-of-bounds Write	05-Jul-2023	9.8	A heap-based buffer overflow vulnerability exists in the Sequence::DrawText functionality of Diagon v1.0.139. A specially crafted network request can lead to a heap buffer overflow. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2023-27390**	N/A	A-DIA-DIAG-240723/133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-Jul-2023	9.8	An access violation vulnerability exists in the GraphPlanar::Write functionality of Diagon v1.0.139. A specially crafted network request can lead to a heap buffer overflow. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2023-31194**	N/A	A-DIA-DIAG-240723/134
Vendor: digitalinspiration					
Product: google_xml_sitemap_for_mobile					
Affected Version(s): * Up to (including) 1.6.1					
Cross-Site Request Forgery (CSRF)	10-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Amit Agarwal Google XML Sitemap for Mobile plugin <= 1.6.1 versions. **CVE ID : CVE-2023-23869**	N/A	A-DIG-GOOG-240723/135
Vendor: Djangoproject					
Product: django					
Affected Version(s): From (including) 3.2 Up to (excluding) 3.2.20					
N/A	03-Jul-2023	7.5	In Django 3.2 before 3.2.20, 4 before 4.1.10, and 4.2 before 4.2.3, EmailValidator and URLValidator are subject to a potential ReDoS (regular expression denial of service) attack via a	https://www.djangoproject.com/weblog/2023/jul/03/security-releases/	A-DJA-DJAN-240723/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			very large number of domain name labels of emails and URLs. **CVE ID : CVE-2023-36053**		
Affected Version(s): From (including) 4.0 Up to (excluding) 4.1.10					
N/A	03-Jul-2023	7.5	In Django 3.2 before 3.2.20, 4 before 4.1.10, and 4.2 before 4.2.3, EmailValidator and URLValidator are subject to a potential ReDoS (regular expression denial of service) attack via a very large number of domain name labels of emails and URLs. **CVE ID : CVE-2023-36053**	https://www.djangoproject.com/weblog/2023/jul/03/security-releases/	A-DJA-DJAN-240723/137
Affected Version(s): From (including) 4.2 Up to (excluding) 4.2.3					
N/A	03-Jul-2023	7.5	In Django 3.2 before 3.2.20, 4 before 4.1.10, and 4.2 before 4.2.3, EmailValidator and URLValidator are subject to a potential ReDoS (regular expression denial of service) attack via a very large number of domain name labels of emails and URLs. **CVE ID : CVE-2023-36053**	https://www.djangoproject.com/weblog/2023/jul/03/security-releases/	A-DJA-DJAN-240723/138
Vendor: drogon					
Product: drogon					
Affected Version(s): *					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	06-Jul-2023	6.1	All versions of the package drogonframework/drogon are vulnerable to HTTP Response Splitting when untrusted user input is used to build header values in the addHeader and addCookie functions. An attacker can add the \r\n (carriage return line feeds) characters to end the HTTP response headers and inject malicious content. **CVE ID : CVE-2023-26137**	N/A	A-DRO-DROG-240723/139
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Jul-2023	4.3	All versions of the package drogonframework/drogon are vulnerable to CRLF Injection when untrusted user input is used to set request headers in the addHeader function. An attacker can add the \r\n (carriage return line feeds) characters and inject additional headers in the request sent. **CVE ID : CVE-2023-26138**	N/A	A-DRO-DROG-240723/140
Vendor: ENG					
Product: knowage					
Affected Version(s): From (including) 6.0.0 Up to (excluding) 8.1.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Jul-2023	6.5	Knowage is the professional open source suite for modern business analytics over traditional sources and big data systems. The endpoint `_/knowage/restful-services/dossier/importTemplateFile_` allows authenticated users to download template hosted on the server. However, starting in the 6.x.x branch and prior to version 8.1.8, the application does not sanitize the `_templateName_ `parameter allowing an attacker to use `*../*` in it, and escaping the directory the template are normally placed and download any file from the system. This vulnerability allows a low privileged attacker to exfiltrate sensitive configuration file. This issue has been patched in Knowage version 8.1.8. **CVE ID : CVE-2023-36819**	N/A	A-ENG-KNOW-240723/141
Vendor: enzipe					
Product: prepost_seo					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	4.8	The PrePost SEO WordPress plugin through 3.0 does not properly sanitize some of its settings, which could allow high-privilege users to perform Stored Cross-Site Scripting (XSS) attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2023-2029**	N/A	A-ENZ-PREP-240723/142
Vendor: ethyca					
Product: fides					
Affected Version(s): * Up to (excluding) 2.15.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jul-2023	7.5	Fides is an open-source privacy engineering platform for managing the fulfillment of data privacy requests in a runtime environment, and the enforcement of privacy regulations in code. A path traversal (directory traversal) vulnerability affects fides versions lower than version `2.15.1`, allowing remote attackers to access arbitrary files on the fides webserver	https://github.com/ethyca/fides/commit/f526d9ffb176006d701493c9d0eff6b4884e811f	A-ETH-FIDE-240723/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			container's filesystem. The vulnerability is patched in fides `2.15.1`. If the Fides webserver API is not directly accessible to attackers and is instead deployed behind a reverse proxy as recommended in Ethyca's security best practice documentation, and the reverse proxy is an AWS application load balancer, the vulnerability can't be exploited by these attackers. An AWS application load balancer will reject this attack with a 400 error. Additionally, any secrets supplied to the container using environment variables rather than a `fides.toml` configuration file are not affected by this vulnerability. **CVE ID : CVE-2023-36827**		
Vendor: eyoucms					
Product: eyoucms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.6.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the custom variables module of eyoucms v1.6.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload. **CVE ID : CVE-2023-37132**	N/A	A-EYO-EYOU-240723/144
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Column management module of eyoucms v1.6.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload. **CVE ID : CVE-2023-37133**	N/A	A-EYO-EYOU-240723/145
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Basic Information module of eyoucms v1.6.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload. **CVE ID : CVE-2023-37134**	N/A	A-EYO-EYOU-240723/146
Improper Neutralization of Input During	06-Jul-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Image Upload module of eyoucms	N/A	A-EYO-EYOU-240723/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			v1.6.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload. **CVE ID : CVE-2023-37135**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Basic Website Information module of eyoucms v1.6.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload. **CVE ID : CVE-2023-37136**	N/A	A-EYO-EYOU-240723/148
Vendor: fit2cloud					
Product: 1panel					
Affected Version(s): * Up to (excluding) 1.3.6					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	8.8	1Panel is an open source Linux server operation and maintenance management panel. Prior to version 1.3.6, an authenticated attacker can craft a malicious payload to achieve command injection when adding container repositories. The vulnerability has been fixed in v1.3.6. **CVE ID : CVE-2023-36457**	https://github.com/1Panel-dev/1Panel/security/advisories/GHSA-q2mx-gpjf-3h8x	A-FIT-1PAN-240723/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	8.8	1Panel is an open source Linux server operation and maintenance management panel. Prior to version 1.3.6, an authenticated attacker can craft a malicious payloads to achieve command injection when entering the container terminal. The vulnerability has been fixed in v1.3.6. **CVE ID : CVE-2023-36458**	https://github.com/1Panel-dev/1Panel/security/advisories/GHSA-7x2c-fgx6-xf9h	A-FIT-1PAN-240723/150
Vendor: food_ordering_system_project					
Product: food_ordering_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jul-2023	7.2	A SQL Injection vulnerability detected in Food Ordering System v1.0 allows attackers to run commands on the database by sending crafted SQL queries to the ID parameter. **CVE ID : CVE-2023-36968**	N/A	A-FOO-FOOD-240723/151
Vendor: fossbilling					
Product: fossbilling					
Affected Version(s): * Up to (excluding) 0.5.4					
Improper Neutralization of Input During	06-Jul-2023	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository	https://huntr.dev/bounties/76a3441d-7f75-4a8d-a7a0-	A-FOS-FOSS-240723/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			fossbilling/fossbilling prior to 0.5.4. **CVE ID : CVE-2023-3521**	95a7f5456eb0, https://github.com/fossbilling/fossbilling/commit/5eb516d4ebcb764db1b2edf9c8d0539e76ebde52	
Vendor: frauscher					
Product: frauscher_diagnostic_system_101					
Affected Version(s): * Up to (including) 1.3.3					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jul-2023	7.5	Frauscher Sensortechnik GmbH FDS001 for FAdC/FAdCi v1.3.3 and all previous versions are vulnerable to a path traversal vulnerability of the web interface by a crafted URL without authentication. This enables an remote attacker to read all files on the filesystem of the FDS001 device. **CVE ID : CVE-2023-2880**	N/A	A-FRA-FRAU-240723/153
Vendor: getoutline					
Product: outline					
Affected Version(s): * Up to (excluding) 0.70.1					
Improper Neutralization of Input During Web Page	07-Jul-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository outline/outline prior to 0.70.1.	https://huntr.dev/bounties/ebd2428a-e2cb-480e-ba37-dd89ad62cf1	A-GET-OUTL-240723/154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			**CVE ID : CVE-2023-3532**	b, https://github.com/outline/outline/commit/9431df45c210e85b77cd27f2ffaf0358b837afa3	
Vendor: gis3w					
Product: g3w-suite					
Affected Version(s): 3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	5.4	A Cross-site scripting (XSS) vulnerability in the content editor in Gis3W g3w-suite 3.5 allows remote authenticated users to inject arbitrary web script or HTML and gain privileges via the description parameter. **CVE ID : CVE-2023-29998**	https://labs.yarix.com/2023/07/gis3w-persistent-xss-in-g3wsuite-3-5-cve-2023-29998/	A-GIS-G3W--240723/155
Vendor: gitea					
Product: gitea					
Affected Version(s): * Up to (excluding) 1.19.4					
URL Redirection to Untrusted Site ('Open Redirect')	05-Jul-2023	4.4	Open Redirect in GitHub repository go-gitea/gitea prior to 1.19.4. **CVE ID : CVE-2023-3515**	https://github.com/go-gitea/gitea/commit/9aaaf980f0ba15611f30568bd67bce3ec12954e2, https://huntr.dev/bounties/e335cd18-bc4d-4585-adb7-	A-GIT-GITE-240723/156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				426c817ed053	
Vendor: Glpi-project					
Product: glpi					
Affected Version(s): From (including) 0.68 Up to (excluding) 10.0.8					
Improper Access Control	05-Jul-2023	6.5	GLPI is a free asset and IT management software package. Versions of the software starting with 0.68 and prior to 10.0.8 have an incorrect rights check on a on a file accessible by an authenticated user. This allows access to the list of all users and their personal information. Users should upgrade to version 10.0.8 to receive a patch. **CVE ID : CVE-2023-34106**	https://github.com/glpi-project/glpi/security/advisories/GHSA-923r-hqh4-wj7c	A-GLP-GLPI-240723/157
Affected Version(s): From (including) 0.80 Up to (excluding) 10.0.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2023	9.8	GLPI is a free asset and IT management software package. Starting in version 0.80 and prior to version 10.0.8, Computer Virtual Machine form and GLPI inventory request can be used to perform a SQL injection attack. Version 10.0.8 has a patch for this issue. As a workaround,	https://github.com/glpi-project/glpi/security/advisories/GHSA-vf5h-jh9q-2gjm	A-GLP-GLPI-240723/158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			one may disable native inventory. **CVE ID : CVE-2023-36808**		
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.0.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2023	9.8	GLPI is a free asset and IT management software package. Starting in version 10.0.0 and prior to version 10.0.8, GLPI inventory endpoint can be used to drive a SQL injection attack. By default, GLPI inventory endpoint requires no authentication. Version 10.0.8 has a patch for this issue. As a workaround, one may disable native inventory. **CVE ID : CVE-2023-35924**	https://github.com/glpi-project/glpi/security/advisories/GHSA-gxh4-j63w-8jmm	A-GLP-GLPI-240723/159
Affected Version(s): From (including) 9.2.0 Up to (excluding) 10.0.8					
Improper Access Control	05-Jul-2023	6.5	GLPI is a free asset and IT management software package. Versions of the software starting with 9.2.0 and prior to 10.0.8 have an incorrect rights check on a on a file accessible by an authenticated user, allows access to the view all KnowbaseItems. Version 10.0.8 has a patch for this issue.	https://github.com/glpi-project/glpi/security/advisories/GHSA-966h-xrf5-pmj4	A-GLP-GLPI-240723/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34107		
Affected Version(s): From (including) 9.4.0 Up to (excluding) 10.0.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	GLPI is a free asset and IT management software package. Starting in version 9.4.0 and prior to version 10.0.8, a malicious link can be crafted by an unauthenticated user that can exploit a reflected XSS in case any authenticated user opens the crafted link. Users should upgrade to version 10.0.8 to receive a patch. **CVE ID : CVE-2023-34244**	https://github.com/glpi-project/glpi/security/advisories/GHSA-p93p-pwg9-w95w	A-GLP-GLPI-240723/161
Affected Version(s): From (including) 9.5.0 Up to (excluding) 10.0.8					
Improper Access Control	05-Jul-2023	8.1	GLPI is a free asset and IT management software package. Starting in version 9.5.0 and prior to version 10.0.8, an incorrect rights check on a on a file accessible by an authenticated user (or not for certain actions), allows a threat actor to interact, modify, or see Dashboard data. Version 10.0.8 contains a patch for this issue.	https://github.com/glpi-project/glpi/security/advisories/GHSA-cjcx-pwcx-v34c	A-GLP-GLPI-240723/162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35939		
Missing Authorization	05-Jul-2023	7.5	GLPI is a free asset and IT management software package. Starting in version 9.5.0 and prior to version 10.0.8, an incorrect rights check on a file allows an unauthenticated user to be able to access dashboards data. Version 10.0.8 contains a patch for this issue. **CVE ID : CVE-2023-35940**	https://github.com/glpi-project/glpi/security/advisories/GHSA-qrh8-rg45-45fw	A-GLP-GLPI-240723/163
Vendor: goauthentik					
Product: authentik					
Affected Version(s): * Up to (excluding) 2023.4.3					
Interpretation Conflict	06-Jul-2023	7.3	authentik is an open-source Identity Provider. Prior to versions 2023.4.3 and 2023.5.5, authentik does not verify the source of the X-Forwarded-For and X-Real-IP headers, both in the Python code and the go code. Only authentik setups that are directly accessible by users without a reverse proxy are susceptible to this. Possible spoofing of IP addresses in logs, downstream	https://github.com/goauthentik/authentik/commit/15026748d19d490eb2baf9a9566ead4f805f7dff, https://github.com/goauthentik/authentik/security/advisories/GHSA-cmxp-jcw7-jjjv	A-GOA-AUTH-240723/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applications proxied by (built in) outpost, IP bypassing in custom flows if used. This poses a possible security risk when someone has flows or policies that check the user's IP address, e.g. when they want to ignore the user's 2 factor authentication when the user is connected to the company network. A second security risk is that the IP addresses in the logfiles and user sessions are not reliable anymore. Anybody can spoof this address and one cannot verify that the user has logged in from the IP address that is in their account's log. A third risk is that this header is passed on to the proxied application behind an outpost. The application may do any kind of verification, logging, blocking or rate limiting based on the IP address, and this IP address can be overridden by		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anybody that want to. Versions 2023.4.3 and 2023.5.5 contain a patch for this issue. **CVE ID : CVE-2023-36456**		
Affected Version(s): From (including) 2023.5.0 Up to (excluding) 2023.5.5					
Interpretation Conflict	06-Jul-2023	7.3	authentik is an open-source Identity Provider. Prior to versions 2023.4.3 and 2023.5.5, authentik does not verify the source of the X-Forwarded-For and X-Real-IP headers, both in the Python code and the go code. Only authentik setups that are directly accessible by users without a reverse proxy are susceptible to this. Possible spoofing of IP addresses in logs, downstream applications proxied by (built in) outpost, IP bypassing in custom flows if used. This poses a possible security risk when someone has flows or policies that check the user's IP address,	https://github.com/goauthentik/authentik/commit/15026748d19d490eb2baf9a9566ead4f805f7dff, https://github.com/goauthentik/authentik/security/advisories/GHSA-cmxp-jcw7-jjjv	A-GOA-AUTH-240723/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			e.g. when they want to ignore the user's 2 factor authentication when the user is connected to the company network. A second security risk is that the IP addresses in the logfiles and user sessions are not reliable anymore. Anybody can spoof this address and one cannot verify that the user has logged in from the IP address that is in their account's log. A third risk is that this header is passed on to the proxied application behind an outpost. The application may do any kind of verification, logging, blocking or rate limiting based on the IP address, and this IP address can be overridden by anybody that want to. Versions 2023.4.3 and 2023.5.5 contain a patch for this issue. **CVE ID : CVE-2023-36456**		
Vendor: Google					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: chrome					
Affected Version(s): * Up to (excluding) 114.0.5735.90					
Out-of-bounds Read	03-Jul-2023	4.6	Out of bounds read in Google Security Processor firmware in Google Chrome on Chrome OS prior to 114.0.5735.90 allowed a local attacker to perform denial of service via physical access to the device. (Chromium security severity: Medium) **CVE ID : CVE-2023-3497**	https://chromereleases.googleblog.com/2023/05/stable-channel-update-for-desktop_30.html	A-GOO-CHRO-240723/166
Vendor: gpac					
Product: gpac					
Affected Version(s): * Up to (including) 2.2.1					
Out-of-bounds Read	06-Jul-2023	7.1	Out-of-bounds Read in GitHub repository gpac/gpac prior to 2.2.2. **CVE ID : CVE-2023-3523**	https://github.com/gpac/gpac/commit/64201a26476c12a7dbdd7ffb5757743af6954db96	A-GPA-GPAC-240723/167
Vendor: gsheetconnector					
Product: cf7_google_sheets_connector					
Affected Version(s): * Up to (excluding) 5.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jul-2023	6.1	The CF7 Google Sheets Connector WordPress plugin before 5.0.2, cf7-google-sheets-connector-pro WordPress plugin through 5.0.2 does not escape a	N/A	A-GSH-CF7_-240723/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-2320**		
Affected Version(s): * Up to (including) 2.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jul-2023	6.1	The CF7 Google Sheets Connector WordPress plugin before 5.0.2, cf7-google-sheets-connector-pro WordPress plugin through 5.0.2 does not escape a parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-2320**	N/A	A-GSH-CF7_-240723/169
Product: elementor_forms_google_sheet_connector					
Affected Version(s): * Up to (excluding) 1.0.7					
Improper Neutralization of Input During Web Page Generation	04-Jul-2023	6.1	The Elementor Forms Google Sheet Connector WordPress plugin before 1.0.7, gsheetconnector-for-elementor-forms-pro WordPress plugin	N/A	A-GSH-ELEM-240723/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			through 1.0.7 does not escape some parameters before outputting them back in attributes, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-2324**		
Affected Version(s): * Up to (including) 1.0.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jul-2023	6.1	The Elementor Forms Google Sheet Connector WordPress plugin before 1.0.7, gsheetconnector-for-elementor-forms-pro WordPress plugin through 1.0.7 does not escape some parameters before outputting them back in attributes, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-2324**	N/A	A-GSH-ELEM-240723/171
Product: ninja_forms_google_sheet_connector					
Affected Version(s): * Up to (excluding) 1.2.7					
Improper Neutralization of Input During	04-Jul-2023	6.1	The Ninja Forms Google Sheet Connector WordPress plugin before 1.2.7,	N/A	A-GSH-NINJ-240723/172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			gsheetconnector-ninja-forms-pro WordPress plugin through 1.2.7 does not escape a parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-2333**		
Affected Version(s): * Up to (including) 1.2.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jul-2023	6.1	The Ninja Forms Google Sheet Connector WordPress plugin before 1.2.7, gsheetconnector-ninja-forms-pro WordPress plugin through 1.2.7 does not escape a parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-2333**	N/A	A-GSH-NINJ-240723/173
Product: wpforms_google_sheet_connector					
Affected Version(s): * Up to (excluding) 3.4.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jul-2023	6.1	The WPForms Google Sheet Connector WordPress plugin before 3.4.6, gsheetconnector-wpforms-pro WordPress plugin through 3.4.6 does not escape a parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-2321**	N/A	A-GSH-WPFO-240723/174
Affected Version(s): * Up to (including) 3.4.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jul-2023	6.1	The WPForms Google Sheet Connector WordPress plugin before 3.4.6, gsheetconnector-wpforms-pro WordPress plugin through 3.4.6 does not escape a parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	N/A	A-GSH-WPFO-240723/175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2321		
Vendor: gzscripts					
Product: availability_booking_calendar_php					
Affected Version(s): 1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	6.1	A vulnerability was found in GZ Scripts Availability Booking Calendar PHP 1.8. It has been classified as problematic. This affects an unknown part of the file load.php of the component HTTP POST Request Handler. The manipulation of the argument cid/first_name/second_name/address_1/country leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-233295. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3543**	N/A	A-GZS-AVAI-240723/176
Product: car_listing_script_php					
Affected Version(s): 1.8					
Improper Neutralization of	10-Jul-2023	6.1	A vulnerability was found in GZ Scripts Car Listing Script	N/A	A-GZS-CAR_-240723/177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			PHP 1.8. It has been declared as problematic. This vulnerability affects unknown code of the file /preview.php. The manipulation of the argument page/sort_by leads to cross site scripting. The attack can be initiated remotely. VDB-233350 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3556**		
Product: event_booking_calendar					
Affected Version(s): 1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	5.4	A vulnerability classified as problematic has been found in GZ Scripts Event Booking Calendar 1.8. Affected is an unknown function of the file /load.php. The manipulation of the argument first_name/second_name/phone/address_1/country leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this	N/A	A-GZS-EVEN-240723/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-233352. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3558**		
Product: gz_e_learning_platform					
Affected Version(s): 1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	6.1	A vulnerability was found in GZ Scripts GZ E Learning Platform 1.8 and classified as problematic. This issue affects some unknown processing of the component URL Parameter Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-233357 was assigned to this vulnerability. **CVE ID : CVE-2023-3563**	N/A	A-GZS-GZ_E-240723/179
Product: gz_forum_script					
Affected Version(s): 1.8					
Improper Neutralization of Input During Web Page	10-Jul-2023	6.1	A vulnerability was found in GZ Scripts GZ Forum Script 1.8 and classified as problematic. Affected by this issue	N/A	A-GZS-GZ_F-240723/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			is some unknown functionality of the file /preview.php. The manipulation of the argument catid/topicid/topic/topic_message/free_name leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-233348. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3554**		
Product: gz_multi_hotel_booking_system					
Affected Version(s): 1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	6.1	A vulnerability was found in GZ Scripts GZ Multi Hotel Booking System 1.8. It has been classified as problematic. Affected is an unknown function of the file /index.php. The manipulation of the argument adults/children/cal_id leads to cross site scripting. It is possible to launch the attack remotely. VDB-233358 is the identifier assigned to this vulnerability.	N/A	A-GZS-GZ_M-240723/181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3564		
Product: php_crm_platform					
Affected Version(s): 1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	6.1	A vulnerability has been found in GZ Scripts PHP CRM Platform 1.8 and classified as problematic. This vulnerability affects unknown code of the file /index.php. The manipulation of the argument action leads to cross site scripting. The attack can be initiated remotely. The identifier of this vulnerability is VDB-233356. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3562**	N/A	A-GZS-PHP_-240723/182
Product: php_gz_appointment_scheduling_script					
Affected Version(s): 1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	6.1	A vulnerability classified as problematic was found in GZ Scripts PHP GZ Appointment Scheduling Script 1.8. Affected by this vulnerability is an unknown functionality of the file /load.php. The	N/A	A-GZS-PHP_-240723/183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the argument first_name/second_name/phone/address_1/country leads to cross site scripting. The attack can be launched remotely. The identifier VDB-233353 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3559**		
Product: php_gz_hotel_booking_script					
Affected Version(s): 1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	6.1	A vulnerability, which was classified as problematic, was found in GZ Scripts PHP GZ Hotel Booking Script 1.8. This affects an unknown part of the file /load.php. The manipulation of the argument first_name/second_name/phone/address_1/country leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-233355. NOTE: The vendor was	N/A	A-GZS-PHP_-240723/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3561**		
Product: php_vacation_rental_script					
Affected Version(s): 1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	6.1	A vulnerability was found in GZ Scripts PHP Vacation Rental Script 1.8. It has been classified as problematic. This affects an unknown part of the file /preview.php. The manipulation of the argument page/layout/sort_by /property_id leads to cross site scripting. It is possible to initiate the attack remotely. The identifier VDB-233349 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3555**	N/A	A-GZS-PHP_-240723/185
Product: property_listing_script					
Affected Version(s): 1.0					
Improper Neutralization of Input	10-Jul-2023	6.1	A vulnerability was found in GZ Scripts Property Listing Script 1.0. It has been	N/A	A-GZS-PROP-240723/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			rated as problematic. This issue affects some unknown processing of the file /preview.php. The manipulation of the argument page/layout/sort_by leads to cross site scripting. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-233351. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3557**		
Product: ticket_booking_script					
Affected Version(s): 1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	6.1	A vulnerability, which was classified as problematic, has been found in GZ Scripts Ticket Booking Script 1.8. Affected by this issue is some unknown functionality of the file /load.php. The manipulation of the argument first_name/second_name/phone/address_1/country leads to cross site scripting. The attack may be launched remotely. VDB-233354 is the	N/A	A-GZS-TICK-240723/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3560**		
Product: time_slot_booking_calendar_php					
Affected Version(s): 1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	6.1	A vulnerability was found in GZ Scripts Time Slot Booking Calendar PHP 1.8. It has been declared as problematic. This vulnerability affects unknown code of the file /load.php. The manipulation of the argument first_name/second_name/phone/address_1/country leads to cross site scripting. The attack can be initiated remotely. The identifier of this vulnerability is VDB-233296. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3544**	N/A	A-GZS-TIME-240723/188
Vendor: hasthemes					
Product: ht_feed					
Affected Version(s): * Up to (excluding) 1.2.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	10-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in HasThemes HT Feed plugin <= 1.2.7 versions. **CVE ID : CVE-2023-23804**	N/A	A-HAS-HT_F-240723/189
Product: ht_menu					
Affected Version(s): * Up to (excluding) 1.2.2					
Cross-Site Request Forgery (CSRF)	11-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in HasThemes HT Menu plugin <= 1.2.1 versions. **CVE ID : CVE-2023-23791**	N/A	A-HAS-HT_M-240723/190
Product: justtables					
Affected Version(s): * Up to (excluding) 1.5.0					
Cross-Site Request Forgery (CSRF)	11-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in HasThemes JustTables plugin <= 1.4.9 versions. **CVE ID : CVE-2023-23803**	N/A	A-HAS-JUST-240723/191
Product: swatchly					
Affected Version(s): * Up to (excluding) 1.2.1					
Cross-Site Request Forgery (CSRF)	11-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in HasThemes Swatchly plugin <= 1.2.0 versions. **CVE ID : CVE-2023-23792**	N/A	A-HAS-SWAT-240723/192
Product: wishsuite					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.3.4					
Cross-Site Request Forgery (CSRF)	11-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in HasTheme WishSuite plugin <= 1.3.3 versions. **CVE ID : CVE-2023-23731**	N/A	A-HAS-WISH-240723/193
Vendor: hostel_management_system_project					
Product: hostel_management_system					
Affected Version(s): 2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	4.8	Cross-Site Scripting (XSS) vulnerability in Hostel Management System v.2.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the add course section. **CVE ID : CVE-2023-36376**	https://medium.com/@ridheshgohil1092/cve-2023-36376-xss-on-hostel-management-system-c6891993527	A-HOS-HOST-240723/194
Vendor: http_headers_project					
Product: http_headers					
Affected Version(s): * Up to (excluding) 1.18.11					
N/A	10-Jul-2023	7.2	This HTTP Headers WordPress plugin before 1.18.11 allows arbitrary data to be written to arbitrary files, leading to a Remote Code Execution vulnerability. **CVE ID : CVE-2023-1208**	N/A	A-HTT-HTTP-240723/195
Vendor: IBM					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: cloud_pak_for_data					
Affected Version(s): 4.6.0					
Allocation of Resources Without Limits or Throttling	10-Jul-2023	7.5	IBM Watson CP4D Data Stores 4.6.0 does not properly allocate resources without limits or throttling which could allow a remote attacker with information specific to the system to cause a denial of service. IBM X-Force ID: 248924. **CVE ID : CVE-2023-27540**	https://www.ibm.com/support/pages/node/7009883, https://exchange.xforce.ibmcloud.com/vulnerabilities/248924	A-IBM-CLOU-240723/196
Product: cognos_analytics_cartridge_for_ibm_cloud_pak_for_data					
Affected Version(s): From (including) 4.0 Up to (excluding) 4.7					
N/A	10-Jul-2023	4.3	IBM Cognos Analytics on Cloud Pak for Data 4.0 could allow an attacker to make system calls that might compromise the security of the containers due to misconfigured security context. IBM X-Force ID: 251465. **CVE ID : CVE-2023-28953**	https://www.ibm.com/support/pages/node/7006413, https://exchange.xforce.ibmcloud.com/vulnerabilities/251465	A-IBM-COGN-240723/197
Product: db2					
Affected Version(s): 10.5.0.11					
Improper Control of Generation of Code	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote	https://exchange.xforce.ibmcloud.com/vulnerabilities/24951	A-IBM-DB2-240723/198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			authenticated attacker to execute arbitrary code via JNDI Injection. By sending a specially crafted request using the property clientRerouteServer ListJNDIName, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249514. **CVE ID : CVE-2023-27867**	4, https://www.ibm.com/support/pages/node/7010029	
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked class instantiation when providing plugin classes. By sending a specially crafted request using the named pluginClassName class, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249516.	https://exchange.xforce.ibmcloud.com/vulnerabilities/249516, https://www.ibm.com/support/pages/node/7010029	A-IBM-DB2-240723/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27868		
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked logger injection. By sending a specially crafted request using the named traceFile property, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249517. **CVE ID : CVE-2023-27869**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249517, https://www.ibm.com/support/pages/node/7010029	A-IBM-DB2-240723/200
Improper Privilege Management	10-Jul-2023	7.8	IBM Db2 on Windows 10.5, 11.1, and 11.5 may be vulnerable to a privilege escalation caused by at least one installed service using an unquoted service path. A local attacker could exploit this vulnerability to gain elevated privileges by inserting an executable file in the path of the affected service. IBM X-Force ID: 249194.	https://www.ibm.com/support/pages/node/7010571, https://exchange.xforce.ibmcloud.com/vulnerabilities/249194	A-IBM-DB2-240723/201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27558		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Jul-2023	7.8	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 db2set is vulnerable to a buffer overflow, caused by improper bounds checking. An attacker could overflow the buffer and execute arbitrary code. IBM X-Force ID: 252184. **CVE ID : CVE-2023-30431**	https://www.ibm.com/support/pages/node/7010565, https://exchange.xforce.ibmcloud.com/vulnerabilities/252184	A-IBM-DB2-240723/202
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253357. **CVE ID : CVE-2023-30445**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253357, https://www.ibm.com/support/pages/node/7010557	A-IBM-DB2-240723/203
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain	https://www.ibm.com/support/pages/node/7010557, https://exchange.xforce.ibmcloud.com/vulnerabi	A-IBM-DB2-240723/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tables. IBM X-Force ID: 253361 . **CVE ID : CVE-2023-30446**	lities/253361	
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253436. **CVE ID : CVE-2023-30447**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253436, https://www.ibm.com/support/pages/node/7010557	A-IBM-DB2-240723/205
N/A	10-Jul-2023	7.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253437. **CVE ID : CVE-2023-30448**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253437, https://www.ibm.com/support/pages/node/7010557	A-IBM-DB2-240723/206
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server)	https://exchange.xforce.ibmcloud.com/vulnerabilities/25343	A-IBM-DB2-240723/207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query. IBM X-Force ID: 253439. **CVE ID : CVE-2023-30449**	9, https://www.ibm.com/support/pages/node/7010557	
Improper Privilege Management	10-Jul-2023	6.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to an information disclosure due to improper privilege management when certain federation features are used. IBM X-Force ID: 252046. **CVE ID : CVE-2023-29256**	https://www.ibm.com/support/pages/node/7010573, https://exchange.xforce.ibmcloud.com/vulnerabilities/252046	A-IBM-DB2-240723/208
Affected Version(s): 11.1					
N/A	10-Jul-2023	4.3	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is vulnerable to insufficient audit logging. IBM X-Force ID: 245918. **CVE ID : CVE-2023-23487**	https://exchange.xforce.ibmcloud.com/vulnerabilities/245918, https://www.ibm.com/support/pages/node/7010567	A-IBM-DB2-240723/209
Affected Version(s): 11.1.4.7					
Improper Control of Generation of Code	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5	https://exchange.xforce.ibmcloud.com/vulnerabi	A-IBM-DB2-240723/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			could allow a remote authenticated attacker to execute arbitrary code via JNDI Injection. By sending a specially crafted request using the property clientRerouteServer ListJNDIName, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249514. **CVE ID : CVE-2023-27867**	lities/249514, https://www.ibm.com/support/pages/node/7010029	
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked class instantiation when providing plugin classes. By sending a specially crafted request using the named pluginClassName class, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249516.	https://exchange.xforce.ibmcloud.com/vulnerabilities/249516, https://www.ibm.com/support/pages/node/7010029	A-IBM-DB2-240723/211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27868		
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked logger injection. By sending a specially crafted request using the named traceFile property, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249517. **CVE ID : CVE-2023-27869**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249517, https://www.ibm.com/support/pages/node/7010029	A-IBM-DB2-240723/212
Improper Privilege Management	10-Jul-2023	7.8	IBM Db2 on Windows 10.5, 11.1, and 11.5 may be vulnerable to a privilege escalation caused by at least one installed service using an unquoted service path. A local attacker could exploit this vulnerability to gain elevated privileges by inserting an executable file in the path of the affected service. IBM X-Force ID: 249194.	https://www.ibm.com/support/pages/node/7010571, https://exchange.xforce.ibmcloud.com/vulnerabilities/249194	A-IBM-DB2-240723/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27558		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Jul-2023	7.8	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 db2set is vulnerable to a buffer overflow, caused by improper bounds checking. An attacker could overflow the buffer and execute arbitrary code. IBM X-Force ID: 252184. **CVE ID : CVE-2023-30431**	https://www.ibm.com/support/pages/node/7010565, https://exchange.xforce.ibmcloud.com/vulnerabilities/252184	A-IBM-DB2-240723/214
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 federated server is vulnerable to a denial of service as the server may crash when using a specially crafted wrapper using certain options. IBM X-Force ID: 253202. **CVE ID : CVE-2023-30442**	https://www.ibm.com/support/pages/node/7010561, https://exchange.xforce.ibmcloud.com/vulnerabilities/253202	A-IBM-DB2-240723/215
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted	https://exchange.xforce.ibmcloud.com/vulnerabilities/253357, https://www.ibm.com/support/page	A-IBM-DB2-240723/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			query on certain tables. IBM X-Force ID: 253357. **CVE ID : CVE-2023-30445**	s/node/7010557	
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253361 . **CVE ID : CVE-2023-30446**	https://www.ibm.com/support/pages/node/7010557, https://exchange.xforce.ibmcloud.com/vulnerabilities/253361	A-IBM-DB2-240723/217
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253436. **CVE ID : CVE-2023-30447**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253436, https://www.ibm.com/support/pages/node/7010557	A-IBM-DB2-240723/218
N/A	10-Jul-2023	7.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server)	https://exchange.xforce.ibmcloud.com/vulnerabilities/253437,	A-IBM-DB2-240723/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253437. **CVE ID : CVE-2023-30448**	https://www.ibm.com/support/pages/node/7010557	
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query. IBM X-Force ID: 253439. **CVE ID : CVE-2023-30449**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253439, https://www.ibm.com/support/pages/node/7010557	A-IBM-DB2-240723/220
Improper Privilege Management	10-Jul-2023	6.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to an information disclosure due to improper privilege management when certain federation features are used. IBM X-Force ID: 252046. **CVE ID : CVE-2023-29256**	https://www.ibm.com/support/pages/node/7010573, https://exchange.xforce.ibmcloud.com/vulnerabilities/252046	A-IBM-DB2-240723/221
Affected Version(s): 11.5					
Improper Control of	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux,	https://exchange.xforce.i	A-IBM-DB2-240723/222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code via JNDI Injection. By sending a specially crafted request using the property clientRerouteServer ListJNDIName, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249514. **CVE ID : CVE-2023-27867**	bmcloud.com/vulnerabilities/249514, https://www.ibm.com/support/pages/node/7010029	
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked class instantiation when providing plugin classes. By sending a specially crafted request using the named pluginClassName class, an attacker could exploit this vulnerability to execute arbitrary code on the system.	https://exchange.xforce.ibmcloud.com/vulnerabilities/249516, https://www.ibm.com/support/pages/node/7010029	A-IBM-DB2-240723/223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 249516. **CVE ID : CVE-2023-27868**		
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked logger injection. By sending a specially crafted request using the named traceFile property, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249517. **CVE ID : CVE-2023-27869**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249517, https://www.ibm.com/support/pages/node/7010029	A-IBM-DB2-240723/224
Improper Privilege Management	10-Jul-2023	7.8	IBM Db2 on Windows 10.5, 11.1, and 11.5 may be vulnerable to a privilege escalation caused by at least one installed service using an unquoted service path. A local attacker could exploit this vulnerability to gain elevated privileges by inserting an executable file in the path of the affected	https://www.ibm.com/support/pages/node/7010571, https://exchange.xforce.ibmcloud.com/vulnerabilities/249194	A-IBM-DB2-240723/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service. IBM X-Force ID: 249194. **CVE ID : CVE-2023-27558**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Jul-2023	7.8	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 db2set is vulnerable to a buffer overflow, caused by improper bounds checking. An attacker could overflow the buffer and execute arbitrary code. IBM X-Force ID: 252184. **CVE ID : CVE-2023-30431**	https://www.ibm.com/support/pages/node/7010565, https://exchange.xforce.ibmcloud.com/vulnerabilities/252184	A-IBM-DB2-240723/226
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 federated server is vulnerable to a denial of service as the server may crash when using a specially crafted wrapper using certain options. IBM X-Force ID: 253202. **CVE ID : CVE-2023-30442**	https://www.ibm.com/support/pages/node/7010561, https://exchange.xforce.ibmcloud.com/vulnerabilities/253202	A-IBM-DB2-240723/227
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to	https://exchange.xforce.ibmcloud.com/vulnerabilities/253357, https://ww	A-IBM-DB2-240723/228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253357. **CVE ID : CVE-2023-30445**	w.ibm.com/support/pages/node/7010557	
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253361 . **CVE ID : CVE-2023-30446**	https://www.ibm.com/support/pages/node/7010557, https://exchange.xforce.ibmcloud.com/vulnerabilities/253361	A-IBM-DB2-240723/229
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253436. **CVE ID : CVE-2023-30447**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253436, https://www.ibm.com/support/pages/node/7010557	A-IBM-DB2-240723/230
N/A	10-Jul-2023	7.5	IBM DB2 for Linux, UNIX and Windows	https://exchange.xforce.ibmcloud.com/vulnerabi	A-IBM-DB2-240723/231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253437. **CVE ID : CVE-2023-30448**	lities/253437, https://www.ibm.com/support/pages/node/7010557	
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query. IBM X-Force ID: 253439. **CVE ID : CVE-2023-30449**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253439, https://www.ibm.com/support/pages/node/7010557	A-IBM-DB2-240723/232
Improper Privilege Management	10-Jul-2023	6.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to an information disclosure due to improper privilege management when certain federation features are used. IBM X-Force ID: 252046. **CVE ID : CVE-2023-29256**	https://www.ibm.com/support/pages/node/7010573, https://exchange.xforce.ibmcloud.com/vulnerabilities/252046	A-IBM-DB2-240723/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Jul-2023	4.3	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is vulnerable to insufficient audit logging. IBM X-Force ID: 245918. **CVE ID : CVE-2023-23487**	https://exchange.xforce.ibmcloud.com/vulnerabilities/245918, https://www.ibm.com/support/pages/node/7010567	A-IBM-DB2-240723/234
Product: watson_cp4d_data_stores					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	10-Jul-2023	7.5	IBM Watson CP4D Data Stores 4.6.0 does not properly allocate resources without limits or throttling which could allow a remote attacker with information specific to the system to cause a denial of service. IBM X-Force ID: 248924. **CVE ID : CVE-2023-27540**	https://www.ibm.com/support/pages/node/7009883, https://exchange.xforce.ibmcloud.com/vulnerabilities/248924	A-IBM-WATS-240723/235
Product: watson_knowledge_catalog_on_cloud_pak_for_data					
Affected Version(s): From (including) 4.0 Up to (excluding) 4.7					
N/A	10-Jul-2023	6.5	IBM Watson Knowledge Catalog on Cloud Pak for Data 4.0 could allow an authenticated user send a specially crafted request that could cause a denial of service. IBM X-Force ID: 251704.	https://www.ibm.com/support/pages/node/7009747, https://exchange.xforce.ibmcloud.com/vulnerabilities/251704	A-IBM-WATS-240723/236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28955		
Affected Version(s): 4.0					
Improper Neutralization of Formula Elements in a CSV File	10-Jul-2023	7.8	IBM Watson Knowledge Catalog on Cloud Pak for Data 4.0 is potentially vulnerable to CSV Injection. A remote attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 251782. **CVE ID : CVE-2023-28958**	https://www.ibm.com/support/pages/node/7009747, https://exchange.xforce.ibmcloud.com/vulnerabilities/251782	A-IBM-WATS-240723/237
Product: websphere_application_server					
Affected Version(s): 8.5.5.23					
Use of a Broken or Risky Cryptographic Algorithm	07-Jul-2023	5.5	IBM WebSphere Application Server 8.5 and 9.0 could provide weaker than expected security, caused by the improper encoding in a local configuration file. IBM X-Force ID: 258637. **CVE ID : CVE-2023-35890**	https://www.ibm.com/support/pages/node/7007857	A-IBM-WEBS-240723/238
Affected Version(s): 9.0.5.15					
Use of a Broken or Risky Cryptograp	07-Jul-2023	5.5	IBM WebSphere Application Server 8.5 and 9.0 could provide weaker than expected security,	https://www.ibm.com/support/pages/node/7007857	A-IBM-WEBS-240723/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
hic Algorithm			caused by the improper encoding in a local configuration file. IBM X-Force ID: 258637. **CVE ID : CVE-2023-35890**		
Affected Version(s): 9.0.5.16					
Use of a Broken or Risky Cryptographic Algorithm	07-Jul-2023	5.5	IBM WebSphere Application Server 8.5 and 9.0 could provide weaker than expected security, caused by the improper encoding in a local configuration file. IBM X-Force ID: 258637. **CVE ID : CVE-2023-35890**	https://www.ibm.com/support/pages/node/7007857	A-IBM-WEBS-240723/240
Vendor: Icinga					
Product: icinga_web_jira_integration					
Affected Version(s): From (including) 1.3.0 Up to (excluding) 1.3.2					
Cross-Site Request Forgery (CSRF)	05-Jul-2023	8.8	icingaweb2-module-jira provides integration with Atlassian Jira. Starting in version 1.3.0 and prior to version 1.3.2, template and field configuration forms perform the deletion action before user input is validated, including the cross site request forgery token. This issue is fixed in version 1.3.2.	https://github.com/Icinga/icingaweb2-module-jira/commit/7f0c53b7a3e87be2f4c2e8840805d7b7c9762424, https://github.com/Icinga/icingaweb2-module-jira/security/advisories/	A-ICI-ICIN-240723/241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			There are no known workarounds. **CVE ID : CVE-2023-30607**	GHSA-gh7w-7f7j-gwp5	
Vendor: image_protector_project					
Product: image_protector					
Affected Version(s): * Up to (including) 1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	4.8	The Image Protector WordPress plugin through 1.1 does not properly sanitize some of its settings, which could allow high-privilege users to perform Stored Cross-Site Scripting (XSS) attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID : CVE-2023-2026**	N/A	A-IMA-IMAG-240723/242
Vendor: incsub					
Product: forminator					
Affected Version(s): * Up to (excluding) 1.24.1					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Jul-2023	3.1	The Forminator WordPress plugin before 1.24.1 does not use an atomic operation to check whether a user has already voted, and then update that information. This leads to a Race Condition that may allow a single user to	N/A	A-INC-FORM-240723/243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vote multiple times on a poll. **CVE ID : CVE-2023-2010**		
Vendor: it-novum					
Product: openitcockpit					
Affected Version(s): * Up to (excluding) 4.6.6					
Sensitive Cookie in HTTPS Session Without 'Secure' Attribute	06-Jul-2023	4.6	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute in GitHub repository it-novum/openitcockpit prior to 4.6.6. **CVE ID : CVE-2023-3520**	https://huntr.dev/bounties/f3b277bb-91db-419e-bcc4-fe0b055d2551, https://github.com/it-novum/openitcockpit/commit/6c717f3c352e55257fc3fef2c5dec111f7d2ee6b	A-IT--OPEN-240723/244
Vendor: ivanti					
Product: endpoint_manager					
Affected Version(s): * Up to (excluding) 2022					
Deserialization of Untrusted Data	01-Jul-2023	9.8	A deserialization of untrusted data exists in EPM 2022 Su3 and all prior versions that allows an unauthenticated user to elevate rights. This exploit could potentially be used in conjunction with other OS (Operating System) vulnerabilities to escalate privileges on the machine or be	https://forums.ivanti.com/s/article/SA-2023-06-20-CVE-2023-28323	A-IVA-ENDP-240723/245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used as a stepping stone to get to other network attached machines. **CVE ID : CVE-2023-28323**		
Affected Version(s): * Up to (including) 2022					
Improper Input Validation	01-Jul-2023	9.8	A improper input validation vulnerability exists in Ivanti Endpoint Manager 2022 and below that could allow privilege escalation or remote code execution. **CVE ID : CVE-2023-28324**	https://forums.ivanti.com/s/article/SA-2023-06-06-CVE-2023-28324	A-IVA-ENDP-240723/246
Affected Version(s): 2022					
Deserialization of Untrusted Data	01-Jul-2023	9.8	A deserialization of untrusted data exists in EPM 2022 Su3 and all prior versions that allows an unauthenticated user to elevate rights. This exploit could potentially be used in conjunction with other OS (Operating System) vulnerabilities to escalate privileges on the machine or be used as a stepping stone to get to other network attached machines.	https://forums.ivanti.com/s/article/SA-2023-06-20-CVE-2023-28323	A-IVA-ENDP-240723/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28323		
Vendor: Jerryscript					
Product: jerryscript					
Affected Version(s): 3.0.0					
N/A	07-Jul-2023	7.5	An issue in JerryscriptProject jerryscript v.3.0.0 allows an attacker to obtain sensitive information via a crafted script to the arrays. **CVE ID : CVE-2023-36201**	N/A	A-JER-JERR-240723/248
Vendor: joinmastodon					
Product: mastodon					
Affected Version(s): * Up to (excluding) 3.5.9					
Allocation of Resources Without Limits or Throttling	06-Jul-2023	7.5	Mastodon is a free, open-source social network server based on ActivityPub. When performing outgoing HTTP queries, Mastodon sets a timeout on individual read operations. Prior to versions 3.5.9, 4.0.5, and 4.1.3, a malicious server can indefinitely extend the duration of the response through slowloris-type attacks. This vulnerability can be used to keep all Mastodon workers busy for an extended	https://github.com/mastodon/mastodon/commit/c5929798bf7e56cc2c79b15bed0c4692ded3dcb6	A-JOI-MAST-240723/249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			duration of time, leading to the server becoming unresponsive. Versions 3.5.9, 4.0.5, and 4.1.3 contain a patch for this issue. **CVE ID : CVE-2023-36461**		
Affected Version(s): From (including) 1.3 Up to (excluding) 3.5.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2023	6.1	Mastodon is a free, open-source social network server based on ActivityPub. Starting in version 1.3 and prior to versions 3.5.9, 4.0.5, and 4.1.3, an attacker using carefully crafted oEmbed data can bypass the HTML sanitization performed by Mastodon and include arbitrary HTML in oEmbed preview cards. This introduces a vector for cross-site scripting (XSS) payloads that can be rendered in the user's browser when a preview card for a malicious link is clicked through. Versions 3.5.9, 4.0.5, and 4.1.3 contain a patch for this issue. **CVE ID : CVE-2023-36459**	https://github.com/mastodon/mastodon/commit/6d8e0fae3e96f3cf4febe03fa7fcf5b95ff761b2	A-JOI-MAST-240723/250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 2.6.0 Up to (excluding) 3.5.9					
N/A	06-Jul-2023	5.4	Mastodon is a free, open-source social network server based on ActivityPub. Starting in version 2.6.0 and prior to versions 3.5.9, 4.0.5, and 4.1.3, an attacker can craft a verified profile link using specific formatting to conceal arbitrary parts of the link, enabling it to appear to link to a different URL altogether. The link is visually misleading, but clicking on it will reveal the actual link. This can still be used for phishing, though, similar to IDN homograph attacks. Versions 3.5.9, 4.0.5, and 4.1.3 contain a patch for this issue. **CVE ID : CVE-2023-36462**	https://github.com/mastodon/mastodon/commit/610731b03dfcadd887078cb0399f4e514aa1931c, https://github.com/mastodon/mastodon/security/advisories/GHSA-55j9-c3mp-6fcq	A-JOI-MAST-240723/251
Affected Version(s): From (including) 3.5.0 Up to (excluding) 3.5.9					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jul-2023	9.9	Mastodon is a free, open-source social network server based on ActivityPub. Starting in version 3.5.0 and prior to versions 3.5.9, 4.0.5, and 4.1.3, attackers using carefully crafted media files can cause	https://github.com/mastodon/mastodon/commit/dc8f1fbd976ae544720a4e07120d9a91b2722440	A-JOI-MAST-240723/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mastodon's media processing code to create arbitrary files at any location. This allows attackers to create and overwrite any file Mastodon has access to, allowing Denial of Service and arbitrary Remote Code Execution. Versions 3.5.9, 4.0.5, and 4.1.3 contain a patch for this issue. **CVE ID : CVE-2023-36460**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jul-2023	9.9	Mastodon is a free, open-source social network server based on ActivityPub. Starting in version 3.5.0 and prior to versions 3.5.9, 4.0.5, and 4.1.3, attackers using carefully crafted media files can cause Mastodon's media processing code to create arbitrary files at any location. This allows attackers to create and overwrite any file Mastodon has access to, allowing Denial of Service and arbitrary Remote Code Execution. Versions 3.5.9, 4.0.5, and 4.1.3	https://github.com/mastodon/mastodon/commit/dc8f1fbd976ae544720a4e07120d9a91b2722440	A-JOI-MAST-240723/253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a patch for this issue. **CVE ID : CVE-2023-36460**		
Allocation of Resources Without Limits or Throttling	06-Jul-2023	7.5	Mastodon is a free, open-source social network server based on ActivityPub. When performing outgoing HTTP queries, Mastodon sets a timeout on individual read operations. Prior to versions 3.5.9, 4.0.5, and 4.1.3, a malicious server can indefinitely extend the duration of the response through slowloris-type attacks. This vulnerability can be used to keep all Mastodon workers busy for an extended duration of time, leading to the server becoming unresponsive. Versions 3.5.9, 4.0.5, and 4.1.3 contain a patch for this issue. **CVE ID : CVE-2023-36461**	https://github.com/mastodon/mastodon/commit/c5929798bf7e56cc2c79b15bed0c4692ded3dcb6	A-JOI-MAST-240723/254
Improper Neutralization of Input During Web Page Generation	06-Jul-2023	6.1	Mastodon is a free, open-source social network server based on ActivityPub. Starting in version 1.3 and prior to versions	https://github.com/mastodon/mastodon/commit/6d8e0fae3e96f3cf4febe03	A-JOI-MAST-240723/255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			3.5.9, 4.0.5, and 4.1.3, an attacker using carefully crafted oEmbed data can bypass the HTML sanitization performed by Mastodon and include arbitrary HTML in oEmbed preview cards. This introduces a vector for cross-site scripting (XSS) payloads that can be rendered in the user's browser when a preview card for a malicious link is clicked through. Versions 3.5.9, 4.0.5, and 4.1.3 contain a patch for this issue. **CVE ID : CVE-2023-36459**	fa7fcf5b95ff761b2	
N/A	06-Jul-2023	5.4	Mastodon is a free, open-source social network server based on ActivityPub. Starting in version 2.6.0 and prior to versions 3.5.9, 4.0.5, and 4.1.3, an attacker can craft a verified profile link using specific formatting to conceal arbitrary parts of the link, enabling it to appear to link to a different URL altogether. The link is visually	https://github.com/mastodon/mastodon/commit/610731b03dfcadd887078cb0399f4e514aa1931c, https://github.com/mastodon/mastodon/security/advisories/GHSA-55j9-c3mp-6fcq	A-JOI-MAST-240723/256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			misleading, but clicking on it will reveal the actual link. This can still be used for phishing, though, similar to IDN homograph attacks. Versions 3.5.9, 4.0.5, and 4.1.3 contain a patch for this issue. **CVE ID : CVE-2023-36462**		
Affected Version(s): From (including) 4.1.0 Up to (excluding) 4.1.3					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jul-2023	9.9	Mastodon is a free, open-source social network server based on ActivityPub. Starting in version 3.5.0 and prior to versions 3.5.9, 4.0.5, and 4.1.3, attackers using carefully crafted media files can cause Mastodon's media processing code to create arbitrary files at any location. This allows attackers to create and overwrite any file Mastodon has access to, allowing Denial of Service and arbitrary Remote Code Execution. Versions 3.5.9, 4.0.5, and 4.1.3 contain a patch for this issue. **CVE ID : CVE-2023-36460**	https://github.com/mastodon/mastodon/commit/dc8f1fbd976ae544720a4e07120d9a91b2722440	A-JOI-MAST-240723/257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	06-Jul-2023	7.5	Mastodon is a free, open-source social network server based on ActivityPub. When performing outgoing HTTP queries, Mastodon sets a timeout on individual read operations. Prior to versions 3.5.9, 4.0.5, and 4.1.3, a malicious server can indefinitely extend the duration of the response through slowloris-type attacks. This vulnerability can be used to keep all Mastodon workers busy for an extended duration of time, leading to the server becoming unresponsive. Versions 3.5.9, 4.0.5, and 4.1.3 contain a patch for this issue. **CVE ID : CVE-2023-36461**	https://github.com/mastodon/mastodon/commit/c5929798bf7e56cc2c79b15bed0c4692ded3dcb6	A-JOI-MAST-240723/258
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2023	6.1	Mastodon is a free, open-source social network server based on ActivityPub. Starting in version 1.3 and prior to versions 3.5.9, 4.0.5, and 4.1.3, an attacker using carefully crafted oEmbed data can	https://github.com/mastodon/mastodon/commit/6d8e0fae3e96f3cf4febe03fa7fcf5b95ff761b2	A-JOI-MAST-240723/259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass the HTML sanitization performed by Mastodon and include arbitrary HTML in oEmbed preview cards. This introduces a vector for cross-site scripting (XSS) payloads that can be rendered in the user's browser when a preview card for a malicious link is clicked through. Versions 3.5.9, 4.0.5, and 4.1.3 contain a patch for this issue. **CVE ID : CVE-2023-36459**		
N/A	06-Jul-2023	5.4	Mastodon is a free, open-source social network server based on ActivityPub. Starting in version 2.6.0 and prior to versions 3.5.9, 4.0.5, and 4.1.3, an attacker can craft a verified profile link using specific formatting to conceal arbitrary parts of the link, enabling it to appear to link to a different URL altogether. The link is visually misleading, but clicking on it will reveal the actual link. This can still be used	https://github.com/mastodon/mastodon/commit/610731b03dfcadd887078cb0399f4e514aa1931c, https://github.com/mastodon/mastodon/security/advisories/GHSA-55j9-c3mp-6fcq	A-JOI-MAST-240723/260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for phishing, though, similar to IDN homograph attacks. Versions 3.5.9, 4.0.5, and 4.1.3 contain a patch for this issue. **CVE ID : CVE-2023-36462**		
Vendor: Kanboard					
Product: kanboard					
Affected Version(s): * Up to (excluding) 1.2.31					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2023	8.8	Kanboard is project management software that focuses on the Kanban methodology. In versions prior to 1.2.31authenticated user is able to perform a SQL Injection, leading to a privilege escalation or loss of confidentiality. It appears that in some insert and update operations, the code improperly uses the PicoDB library to update/insert new information. Version 1.2.31 contains a fix for this issue. **CVE ID : CVE-2023-36813**	https://github.com/kanboard/kanboard/commit/25b93343baeaf8ad018dcd87b094e47a5c6a3e0a	A-KAN-KANB-240723/261
Vendor: kerawen					
Product: omnichannel_stocks					
Affected Version(s): * Up to (excluding) 1.4.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jul-2023	9.8	SQL injection vulnerability found in PrestaShop lekerawen_ocs before v.1.4.1 allow a remote attacker to gain privileges via the KerawenHelper::setCartOperationInfo, and KerawenHelper::resetCheckoutSessionData components. **CVE ID : CVE-2023-27845**	https://security.friendsofpresta.org/modules/2023/07/06/kerawen_ocs.html	A-KER-OMNI-240723/262
Vendor: kingstemple					
Product: the_king\'s_temple_church_website					
Affected Version(s): 0.1.0					
Exposure of Sensitive Information to an Unauthorized Actor	03-Jul-2023	9.1	`tktchurch/website` contains the codebase for The King's Temple Church website. In version 0.1.0, a Stripe API key was found in the public code repository of the church's project. This sensitive information was unintentionally committed and subsequently exposed in the codebase. If an unauthorized party gains access to this key, they could potentially carry out transactions on behalf of the	N/A	A-KIN-THE_-240723/263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			organization, leading to financial losses. Additionally, they could access sensitive customer information, leading to privacy violations and potential legal implications. The affected component is the codebase of our project, specifically the file(s) where the Stripe API key is embedded. The key should have been stored securely, and not committed to the codebase. The maintainers plan to revoke the leaked Stripe API key immediately, generate a new one, and not commit the key to the codebase. **CVE ID : CVE-2023-36817**		
Vendor: kiwitcms					
Product: kiwi_tcms					
Affected Version(s): * Up to (excluding) 12.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	5.4	Kiwi TCMS, an open source test management system allows users to upload attachments to test plans, test cases, etc. Versions of Kiwi TCMS prior to 12.5 had introduced changes which were meant to	https://www.github.com/kiwitcms/kiwi/commit/195ea53eaaf360c19227c864cc0fe58910032c3c, https://www.github.com/kiwitcms	A-KIW-KIWI-240723/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			serve all uploaded files as plain text in order to prevent browsers from executing potentially dangerous files when such files are accessed directly. The previous Nginx configuration was incorrect allowing certain browsers like Firefox to ignore the `Content-Type: text/plain` header on some occasions thus allowing potentially dangerous scripts to be executed. Additionally, file upload validators and parts of the HTML rendering code had been found to require additional sanitation and improvements. Version 12.5 fixes this vulnerability with updated Nginx content type configuration, improved file upload validation code to prevent more potentially dangerous uploads, and Sanitization of test plan names used in the `tree_view_html()` function.	/kiwi/commit/ffb00450be52fe11a82a2507632c2328cae4ec9d, https://github.com/kiwitcms/Kiwi/security/advisories/GHSA-jpgw-2r9m-8qfw	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36809		
Vendor: Kodi					
Product: kodi					
Affected Version(s): * Up to (including) 19.5					
Divide By Zero	05-Jul-2023	5.5	A divide by zero issue discovered in Kodi Home Theater Software 19.5 and earlier allows attackers to cause a denial of service via use of crafted mp3 file. **CVE ID : CVE-2023-30207**	https://github.com/xbmc/xbmc/pull/22391, https://github.com/xbmc/xbmc/commit/dbc00c500f4c4830049cc040a61c439c580eea73	A-KOD-KODI-240723/265
Vendor: Kubernetes					
Product: kubernetes					
Affected Version(s): * Up to (including) 1.24.14					
N/A	03-Jul-2023	6.5	Users may be able to launch containers using images that are restricted by ImagePolicyWebhook when using ephemeral containers. Kubernetes clusters are only affected if the ImagePolicyWebhook admission plugin is used together with ephemeral containers. **CVE ID : CVE-2023-2727**	N/A	A-KUB-KUBE-240723/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Jul-2023	6.5	Users may be able to launch containers that bypass the mountable secrets policy enforced by the ServiceAccount admission plugin when using ephemeral containers. The policy ensures pods running with a service account may only reference secrets specified in the service account's secrets field. Kubernetes clusters are only affected if the ServiceAccount admission plugin and the `kubernetes.io/enforce-mountable-secrets` annotation are used together with ephemeral containers. **CVE ID : CVE-2023-2728**	N/A	A-KUB-KUBE-240723/267
Affected Version(s): From (including) 1.25.0 Up to (including) 1.25.10					
N/A	03-Jul-2023	6.5	Users may be able to launch containers using images that are restricted by ImagePolicyWebhook when using ephemeral containers. Kubernetes clusters	N/A	A-KUB-KUBE-240723/268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are only affected if the ImagePolicyWebhook admission plugin is used together with ephemeral containers. **CVE ID : CVE-2023-2727**		
N/A	03-Jul-2023	6.5	Users may be able to launch containers that bypass the mountable secrets policy enforced by the ServiceAccount admission plugin when using ephemeral containers. The policy ensures pods running with a service account may only reference secrets specified in the service account's secrets field. Kubernetes clusters are only affected if the ServiceAccount admission plugin and the `kubernetes.io/enforce-mountable-secrets` annotation are used together with ephemeral containers.	N/A	A-KUB-KUBE-240723/269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2728		
Affected Version(s): From (including) 1.26.0 Up to (including) 1.26.5					
N/A	03-Jul-2023	6.5	Users may be able to launch containers using images that are restricted by ImagePolicyWebhook when using ephemeral containers. Kubernetes clusters are only affected if the ImagePolicyWebhook admission plugin is used together with ephemeral containers. **CVE ID : CVE-2023-2727**	N/A	A-KUB-KUBE-240723/270
N/A	03-Jul-2023	6.5	Users may be able to launch containers that bypass the mountable secrets policy enforced by the ServiceAccount admission plugin when using ephemeral containers. The policy ensures pods running with a service account may only reference secrets specified in the service account's secrets field. Kubernetes clusters are only affected if	N/A	A-KUB-KUBE-240723/271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the ServiceAccount admission plugin and the `kubernetes.io/enforce-mountable-secrets` annotation are used together with ephemeral containers. **CVE ID : CVE-2023-2728**		
Affected Version(s): From (including) 1.27.0 Up to (including) 1.27.2					
N/A	03-Jul-2023	6.5	Users may be able to launch containers using images that are restricted by ImagePolicyWebhook when using ephemeral containers. Kubernetes clusters are only affected if the ImagePolicyWebhook admission plugin is used together with ephemeral containers. **CVE ID : CVE-2023-2727**	N/A	A-KUB-KUBE-240723/272
N/A	03-Jul-2023	6.5	Users may be able to launch containers that bypass the mountable secrets policy enforced by the ServiceAccount admission plugin	N/A	A-KUB-KUBE-240723/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when using ephemeral containers. The policy ensures pods running with a service account may only reference secrets specified in the service account's secrets field. Kubernetes clusters are only affected if the ServiceAccount admission plugin and the `kubernetes.io/enforce-mountable-secrets` annotation are used together with ephemeral containers. **CVE ID : CVE-2023-2728**		
Vendor: langchain					
Product: langchain					
Affected Version(s): 0.0.199					
N/A	03-Jul-2023	9.8	An issue in langchain v.0.0.199 allows an attacker to execute arbitrary code via the PALChain in the python exec method. **CVE ID : CVE-2023-36258**	N/A	A-LAN-LANG-240723/274
Affected Version(s): 0.0.64					
Improper Neutralization of Special	06-Jul-2023	9.8	An issue in langchain v.0.0.64 allows a remote attacker to execute arbitrary	https://github.com/hwchase17/langc	A-LAN-LANG-240723/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			code via the PALChain parameter in the Python exec method. **CVE ID : CVE-2023-36188**	hain/pull/6003	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jul-2023	7.5	SQL injection vulnerability in langchain v.0.0.64 allows a remote attacker to obtain sensitive information via the SQLDatabaseChain component. **CVE ID : CVE-2023-36189**	https://github.com/hwchase17/langchain/pull/6051	A-LAN-LANG-240723/276
Vendor: lineagrafica					
Product: lgdetailedorder					
Affected Version(s): * Up to (excluding) 1.1.21					
Missing Authorization	06-Jul-2023	7.5	In the module "Detailed Order" (lgdetailedorder) in version up to 1.1.20 from Linea Grafica for PrestaShop, a guest can download personal informations without restriction formatted in json. **CVE ID : CVE-2023-30195**	N/A	A-LIN-LGDE-240723/277
Vendor: Linuxfoundation					
Product: yocto					
Affected Version(s): 4.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664741; Issue ID: ALPS07664741. **CVE ID : CVE-2023-20689**	https://corp.mediatek.com/product-security-bulletin/July-2023	A-LIN-YOCT-240723/278
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664735; Issue ID: ALPS07664735. **CVE ID : CVE-2023-20690**	https://corp.mediatek.com/product-security-bulletin/July-2023	A-LIN-YOCT-240723/279
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2023	A-LIN-YOCT-240723/280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07664731; Issue ID: ALPS07664731. **CVE ID : CVE-2023-20691**		
Improper Handling of Exceptional Conditions	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664720; Issue ID: ALPS07664720. **CVE ID : CVE-2023-20692**	https://corp.mediatek.com/product-security-bulletin/July-2023	A-LIN-YOCT-240723/281
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664711; Issue ID: ALPS07664711. **CVE ID : CVE-2023-20693**	https://corp.mediatek.com/product-security-bulletin/July-2023	A-LIN-YOCT-240723/282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: lionscripts					
Product: ip_blocker_lite					
Affected Version(s): * Up to (including) 11.1.1					
Cross-Site Request Forgery (CSRF)	10-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in LionScripts.Com LionScripts: IP Blocker Lite plugin <= 11.1.1 versions. **CVE ID : CVE-2023-23993**	N/A	A-LIO-IP_B-240723/283
Vendor: lws					
Product: lws_cleaner					
Affected Version(s): * Up to (excluding) 2.3.1					
Cross-Site Request Forgery (CSRF)	11-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in LWS Cleaner plugin <= 2.3.0 versions. **CVE ID : CVE-2023-35781**	N/A	A-LWS-LWS_-240723/284
Product: lws_tools					
Affected Version(s): * Up to (excluding) 2.4.2					
Cross-Site Request Forgery (CSRF)	11-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in LWS LWS Tools plugin <= 2.4.1 versions. **CVE ID : CVE-2023-35774**	N/A	A-LWS-LWS_-240723/285
Vendor: madefornet					
Product: http_debugger					
Affected Version(s): * Up to (including) 9.12					
Concurrent Execution using Shared	05-Jul-2023	5.3	In MADEFORNET HTTP Debugger through 9.12, the Windows service	N/A	A-MAD-HTTP-240723/286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			does not set the seclevel registry key before launching the driver. Thus, it is possible for an unprivileged application to obtain a handle to the NetFilterSDK wrapper before the service obtains exclusive access. **CVE ID : CVE-2023-35863**		
Vendor: magenet					
Product: website_monetization					
Affected Version(s): * Up to (including) 1.0.29.1					
Cross-Site Request Forgery (CSRF)	10-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in MageNet Website Monetization by MageNet plugin <= 1.0.29.1 versions. **CVE ID : CVE-2023-22673**	N/A	A-MAG-WEBS-240723/287
Vendor: Maxsite					
Product: maxsite_cms					
Affected Version(s): 108.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jul-2023	6.1	Cross Site Scripting vulnerability in Maxsite CMS v.108.7 allows a remote attacker to execute arbitrary code via the f_content parameter in the admin/page_new file.	https://github.com/maxsite/cms/issues/500	A-MAX-MAXS-240723/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36291		
Vendor: mechanicalsoup_project					
Product: mechanicalsoup					
Affected Version(s): * Up to (excluding) 1.3.0					
Improper Input Validation	05-Jul-2023	7.5	MechanicalSoup is a Python library for automating interaction with websites. Starting in version 0.2.0 and prior to version 1.3.0, a malicious web server can read arbitrary files on the client using a `<input type="file" ...>` inside HTML form. All users of MechanicalSoup's form submission are affected, unless they took very specific (and manual) steps to reset HTML form field values. Version 1.3.0 contains a patch for this issue. **CVE ID : CVE-2023-34457**	https://github.com/MechanicalSoup/MechanicalSoup/security/advisories/GHSA-x456-3ccm-m6j4, https://github.com/MechanicalSoup/MechanicalSoup/commit/d57c4a269bba3b9a0c5bfa20292955b849006d9e	A-MEC-MECH-240723/289
Vendor: metersphere					
Product: metersphere					
Affected Version(s): * Up to (excluding) 2.10.2					
Missing Authorization	06-Jul-2023	8.8	Metersphere is an open source continuous testing platform. In versions prior to 2.10.2 LTS, some key APIs in Metersphere lack permission checks. This allows ordinary	N/A	A-MET-METE-240723/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			users to execute APIs that can only be executed by space administrators or project administrators. For example, ordinary users can be updated as space administrators. Version 2.10.2 LTS has a patch for this issue. **CVE ID : CVE-2023-35937**		
Vendor: Microsoft					
Product: .net					
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.0.20					
N/A	11-Jul-2023	8.1	.NET and Visual Studio Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33127	A-MIC-.NET-240723/291
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.9					
N/A	11-Jul-2023	8.1	.NET and Visual Studio Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33127	A-MIC-.NET-240723/292
Product: 365_apps					
Affected Version(s): -					
N/A	11-Jul-2023	9.6	Microsoft Office Security Feature Bypass Vulnerability **CVE ID : CVE-2023-33150**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33150	A-MIC-365_-240723/293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	8.8	Microsoft Outlook Remote Code Execution Vulnerability **CVE ID : CVE-2023-33153**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33153	A-MIC-365_-240723/294
N/A	11-Jul-2023	8.8	Microsoft Outlook Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35311**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35311	A-MIC-365_-240723/295
N/A	11-Jul-2023	7.8	Microsoft Office Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33148**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33148	A-MIC-365_-240723/296
N/A	11-Jul-2023	7.8	Microsoft Office Graphics Remote Code Execution Vulnerability **CVE ID : CVE-2023-33149**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33149	A-MIC-365_-240723/297
N/A	11-Jul-2023	7.8	Microsoft ActiveX Remote Code Execution Vulnerability **CVE ID : CVE-2023-33152**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33152	A-MIC-365_-240723/298
N/A	11-Jul-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-33158**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33158	A-MIC-365_-240723/299
N/A	11-Jul-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulner	A-MIC-365_-240723/300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33161	ability/CVE-2023-33161	
N/A	11-Jul-2023	6.5	Microsoft Outlook Spoofing Vulnerability **CVE ID : CVE-2023-33151**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33151	A-MIC-365_-240723/301
N/A	11-Jul-2023	5.5	Microsoft Excel Information Disclosure Vulnerability **CVE ID : CVE-2023-33162**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33162	A-MIC-365_-240723/302
Product: dynamics_365					
Affected Version(s): From (including) 9.0 Up to (excluding) 9.0.47.08					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2023	8.2	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID : CVE-2023-35335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35335	A-MIC-DYNA-240723/303
Affected Version(s): From (including) 9.1 Up to (excluding) 9.1.18.22					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-2023	8.2	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID : CVE-2023-35335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35335	A-MIC-DYNA-240723/304
Product: malware_protection_engine					
Affected Version(s): * Up to (excluding) 1.1.23050.3					
N/A	11-Jul-2023	7	Microsoft Defender Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-	A-MIC-MALW-240723/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33156	guide/vulnerability/CVE-2023-33156	
Product: office					
Affected Version(s): -					
N/A	11-Jul-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-33158**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33158	A-MIC-OFFI-240723/306
Affected Version(s): 2013					
N/A	11-Jul-2023	8.8	Microsoft Outlook Remote Code Execution Vulnerability **CVE ID : CVE-2023-33153**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33153	A-MIC-OFFI-240723/307
N/A	11-Jul-2023	7.8	Microsoft Office Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33148**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33148	A-MIC-OFFI-240723/308
N/A	11-Jul-2023	7.8	Microsoft Office Graphics Remote Code Execution Vulnerability **CVE ID : CVE-2023-33149**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33149	A-MIC-OFFI-240723/309
N/A	11-Jul-2023	7.8	Microsoft ActiveX Remote Code Execution Vulnerability **CVE ID : CVE-2023-33152**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33152	A-MIC-OFFI-240723/310
N/A	11-Jul-2023	6.5	Microsoft Outlook Spoofing Vulnerability	https://msrc.microsoft.com/update-guide/vulner	A-MIC-OFFI-240723/311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33151	ability/CVE-2023-33151	
N/A	11-Jul-2023	5.5	Microsoft Excel Information Disclosure Vulnerability **CVE ID : CVE-2023-33162**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33162	A-MIC-OFFI-240723/312
Affected Version(s): 2016					
N/A	11-Jul-2023	8.8	Microsoft Outlook Remote Code Execution Vulnerability **CVE ID : CVE-2023-33153**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33153	A-MIC-OFFI-240723/313
N/A	11-Jul-2023	7.8	Microsoft Office Graphics Remote Code Execution Vulnerability **CVE ID : CVE-2023-33149**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33149	A-MIC-OFFI-240723/314
N/A	11-Jul-2023	7.8	Microsoft ActiveX Remote Code Execution Vulnerability **CVE ID : CVE-2023-33152**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33152	A-MIC-OFFI-240723/315
N/A	11-Jul-2023	6.5	Microsoft Outlook Spoofing Vulnerability **CVE ID : CVE-2023-33151**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33151	A-MIC-OFFI-240723/316
N/A	11-Jul-2023	5.5	Microsoft Excel Information Disclosure Vulnerability **CVE ID : CVE-2023-33162**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33162	A-MIC-OFFI-240723/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2019					
N/A	11-Jul-2023	9.6	Microsoft Office Security Feature Bypass Vulnerability **CVE ID : CVE-2023-33150**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33150	A-MIC-OFFI-240723/318
N/A	11-Jul-2023	8.8	Microsoft Outlook Remote Code Execution Vulnerability **CVE ID : CVE-2023-33153**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33153	A-MIC-OFFI-240723/319
N/A	11-Jul-2023	8.8	Microsoft Outlook Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35311**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35311	A-MIC-OFFI-240723/320
N/A	11-Jul-2023	7.8	Microsoft Office Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33148**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33148	A-MIC-OFFI-240723/321
N/A	11-Jul-2023	7.8	Microsoft Office Graphics Remote Code Execution Vulnerability **CVE ID : CVE-2023-33149**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33149	A-MIC-OFFI-240723/322
N/A	11-Jul-2023	7.8	Microsoft ActiveX Remote Code Execution Vulnerability **CVE ID : CVE-2023-33152**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33152	A-MIC-OFFI-240723/323
N/A	11-Jul-2023	7.8	Microsoft Excel Remote Code	https://msrc.microsoft.com/update-guide/vulner	A-MIC-OFFI-240723/324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-33158**	ability/CVE-2023-33158	
N/A	11-Jul-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-33161**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33161	A-MIC-OFFI-240723/325
N/A	11-Jul-2023	6.5	Microsoft Outlook Spoofing Vulnerability **CVE ID : CVE-2023-33151**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33151	A-MIC-OFFI-240723/326
N/A	11-Jul-2023	5.5	Microsoft Excel Information Disclosure Vulnerability **CVE ID : CVE-2023-33162**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33162	A-MIC-OFFI-240723/327
Affected Version(s): 2021					
N/A	11-Jul-2023	9.6	Microsoft Office Security Feature Bypass Vulnerability **CVE ID : CVE-2023-33150**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33150	A-MIC-OFFI-240723/328
N/A	11-Jul-2023	8.8	Microsoft Outlook Remote Code Execution Vulnerability **CVE ID : CVE-2023-33153**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33153	A-MIC-OFFI-240723/329
N/A	11-Jul-2023	7.8	Microsoft Office Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33148**	https://msrc.microsoft.com/update-guide/vulner	A-MIC-OFFI-240723/330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ability/CVE-2023-33148	
N/A	11-Jul-2023	7.8	Microsoft Office Graphics Remote Code Execution Vulnerability **CVE ID : CVE-2023-33149**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33149	A-MIC-OFFI-240723/331
N/A	11-Jul-2023	7.8	Microsoft ActiveX Remote Code Execution Vulnerability **CVE ID : CVE-2023-33152**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33152	A-MIC-OFFI-240723/332
N/A	11-Jul-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-33158**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33158	A-MIC-OFFI-240723/333
N/A	11-Jul-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-33161**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33161	A-MIC-OFFI-240723/334
N/A	11-Jul-2023	6.5	Microsoft Outlook Spoofing Vulnerability **CVE ID : CVE-2023-33151**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33151	A-MIC-OFFI-240723/335
N/A	11-Jul-2023	5.5	Microsoft Excel Information Disclosure Vulnerability **CVE ID : CVE-2023-33162**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33162	A-MIC-OFFI-240723/336
Product: office_long_term_servicing_channel					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2021					
N/A	11-Jul-2023	8.8	Microsoft Outlook Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35311**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35311	A-MIC-OFFI-240723/337
Product: office_online_server					
Affected Version(s): -					
N/A	11-Jul-2023	5.5	Microsoft Excel Information Disclosure Vulnerability **CVE ID : CVE-2023-33162**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33162	A-MIC-OFFI-240723/338
Product: outlook					
Affected Version(s): 2013					
N/A	11-Jul-2023	8.8	Microsoft Outlook Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35311**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35311	A-MIC-OUTL-240723/339
Affected Version(s): 2016					
N/A	11-Jul-2023	8.8	Microsoft Outlook Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35311**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35311	A-MIC-OUTL-240723/340
Product: paint_3d					
Affected Version(s): * Up to (excluding) 6.2305.16087.0					
N/A	11-Jul-2023	7.8	Paint 3D Remote Code Execution Vulnerability **CVE ID : CVE-2023-32047**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32047	A-MIC-PAIN-240723/341
Product: pandocupload					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.0.1					
N/A	11-Jul-2023	7.5	MediaWiki PandocUpload Extension Remote Code Execution Vulnerability **CVE ID : CVE-2023-35333**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35333	A-MIC-PAND-240723/342
Product: power_apps					
Affected Version(s): * Up to (excluding) 9.2.23042					
N/A	11-Jul-2023	5.4	Microsoft Power Apps (online) Spoofing Vulnerability **CVE ID : CVE-2023-32052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32052	A-MIC-POWE-240723/343
Product: raw_image_extension					
Affected Version(s): * Up to (excluding) 2.0.61662.0					
N/A	11-Jul-2023	7.8	Raw Image Extension Remote Code Execution Vulnerability **CVE ID : CVE-2023-32051**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32051	A-MIC-RAW_-240723/344
Affected Version(s): * Up to (excluding) 2.1.61661.0					
N/A	11-Jul-2023	7.8	Raw Image Extension Remote Code Execution Vulnerability **CVE ID : CVE-2023-32051**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32051	A-MIC-RAW_-240723/345
Product: sharepoint_server					
Affected Version(s): -					
N/A	11-Jul-2023	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulner	A-MIC-SHAR-240723/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33134	ability/CVE-2023-33134	
N/A	11-Jul-2023	8.8	Microsoft SharePoint Remote Code Execution Vulnerability **CVE ID : CVE-2023-33157**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33157	A-MIC-SHAR-240723/347
N/A	11-Jul-2023	8.8	Microsoft SharePoint Server Spoofing Vulnerability **CVE ID : CVE-2023-33159**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33159	A-MIC-SHAR-240723/348
N/A	11-Jul-2023	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-33160**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33160	A-MIC-SHAR-240723/349
Affected Version(s): 2016					
N/A	11-Jul-2023	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-33134**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33134	A-MIC-SHAR-240723/350
N/A	11-Jul-2023	8.8	Microsoft SharePoint Remote Code Execution Vulnerability **CVE ID : CVE-2023-33157**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33157	A-MIC-SHAR-240723/351
N/A	11-Jul-2023	8.8	Microsoft SharePoint Server Spoofing Vulnerability **CVE ID : CVE-2023-33159**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33159	A-MIC-SHAR-240723/352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-33160**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33160	A-MIC-SHAR-240723/353
Affected Version(s): 2019					
N/A	11-Jul-2023	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-33134**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33134	A-MIC-SHAR-240723/354
N/A	11-Jul-2023	8.8	Microsoft SharePoint Remote Code Execution Vulnerability **CVE ID : CVE-2023-33157**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33157	A-MIC-SHAR-240723/355
N/A	11-Jul-2023	8.8	Microsoft SharePoint Server Spoofing Vulnerability **CVE ID : CVE-2023-33159**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33159	A-MIC-SHAR-240723/356
N/A	11-Jul-2023	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-33160**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33160	A-MIC-SHAR-240723/357
Product: visual_studio_2022					
Affected Version(s): 17.3					
N/A	11-Jul-2023	8.1	.NET and Visual Studio Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33127	A-MIC-VISU-240723/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.23					
N/A	11-Jul-2023	8.1	.NET and Visual Studio Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33127	A-MIC-VISU-240723/359
Affected Version(s): From (including) 17.2.0 Up to (excluding) 17.2.17					
N/A	11-Jul-2023	8.1	.NET and Visual Studio Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33127	A-MIC-VISU-240723/360
Affected Version(s): From (including) 17.4.0 Up to (excluding) 17.4.9					
N/A	11-Jul-2023	8.1	.NET and Visual Studio Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33127	A-MIC-VISU-240723/361
Affected Version(s): From (including) 17.6.0 Up to (excluding) 17.6.5					
N/A	11-Jul-2023	8.1	.NET and Visual Studio Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33127**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33127	A-MIC-VISU-240723/362
Product: windows_admin_center					
Affected Version(s): * Up to (excluding) 2306					
N/A	11-Jul-2023	6.8	Windows Admin Center Spoofing Vulnerability **CVE ID : CVE-2023-29347**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29347	A-MIC-WIND-240723/363
Product: word					
Affected Version(s): 2013					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	9.6	Microsoft Office Security Feature Bypass Vulnerability **CVE ID : CVE-2023-33150**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33150	A-MIC-WORD-240723/364
Affected Version(s): 2016					
N/A	11-Jul-2023	9.6	Microsoft Office Security Feature Bypass Vulnerability **CVE ID : CVE-2023-33150**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33150	A-MIC-WORD-240723/365
Vendor: milesight					
Product: milesightvpn					
Affected Version(s): 2.0.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jul-2023	9.8	A sql injection vulnerability exists in the requestHandlers.js LoginAuth functionality of Milesight VPN v2.0.2. A specially-crafted network request can lead to authentication bypass. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2023-22319**	N/A	A-MIL-MILE-240723/366
Use of Hard-coded Cryptographic Key	06-Jul-2023	9.8	An authentication bypass vulnerability exists in the requestHandlers.js verifyToken functionality of Milesight VPN v2.0.2. A specially-crafted	N/A	A-MIL-MILE-240723/367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network request can lead to authentication bypass. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2023-22844**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jul-2023	8.1	An os command injection vulnerability exists in the liburvpn.so create_private_key functionality of Milesight VPN v2.0.2. A specially-crafted network request can lead to command execution. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2023-22371**	N/A	A-MIL-MILE-240723/368
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jul-2023	7.5	A directory traversal vulnerability exists in the server.js start functionality of Milesight VPN v2.0.2. A specially-crafted network request can lead to arbitrary file read. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2023-23907**	N/A	A-MIL-MILE-240723/369
Improper Neutralizat	06-Jul-2023	4.7	Cross-site scripting (xss) vulnerabilities	N/A	A-MIL-MILE-240723/370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Script-Related HTML Tags in a Web Page (Basic XSS)			exist in the requestHandlers.js detail_device functionality of Milesight VPN v2.0.2. A specially-crafted HTTP request can lead to arbitrary Javascript code injection. An attacker can send an HTTP request to trigger these vulnerabilities.This XSS is exploited through the name field of the database. **CVE ID : CVE-2023-24496**		
Vendor: Mozilla					
Product: firefox					
Affected Version(s): * Up to (excluding) 115.0					
Use After Free	05-Jul-2023	8.8	An attacker could have triggered a use-after-free condition when creating a WebRTC connection over HTTPS. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37201**	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	A-MOZ-FIRE-240723/371
Use After Free	05-Jul-2023	8.8	Cross-compartment wrappers wrapping a scripted proxy could have caused objects from other	https://www.mozilla.org/security/advisories/mfsa2023-23/,	A-MOZ-FIRE-240723/372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compartments to be stored in the main compartment resulting in a use-after-free. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37202**	https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	
Use After Free	05-Jul-2023	8.8	A use-after-free condition existed in `NotifyOnHistoryReload` where a `LoadingSessionHistoryEntry` object was freed and a reference to that object remained. This resulted in a potentially exploitable condition when the reference to that object was later reused. This vulnerability affects Firefox < 115. **CVE ID : CVE-2023-37209**	https://www.mozilla.org/security/advisories/mfsa2023-22/	A-MOZ-FIRE-240723/373
Out-of-bounds Write	05-Jul-2023	8.8	Memory safety bugs present in Firefox 114, Firefox ESR 102.12, and Thunderbird 102.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.or	A-MOZ-FIRE-240723/374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to run arbitrary code. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37211**	g/security/advisories/mfsa2023-24/	
Out-of-bounds Write	05-Jul-2023	8.8	Memory safety bugs present in Firefox 114. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 115. **CVE ID : CVE-2023-37212**	https://www.mozilla.org/security/advisories/mfsa2023-22/	A-MOZ-FIRE-240723/375
N/A	05-Jul-2023	7.8	Insufficient validation in the Drag and Drop API in conjunction with social engineering, may have allowed an attacker to trick end-users into creating a shortcut to local system files. This could have been leveraged to execute arbitrary code. This vulnerability affects Firefox < 115. **CVE ID : CVE-2023-37203**	https://www.mozilla.org/security/advisories/mfsa2023-22/	A-MOZ-FIRE-240723/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Jul-2023	7.8	When opening Diagcab files, Firefox did not warn the user that these files may contain malicious code. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37208**	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	A-MOZ-FIRE-240723/377
Missing Authorization	05-Jul-2023	6.5	When Firefox is configured to block storage of all cookies, it was still possible to store data in localstorage by using an iframe with a source of 'about:blank'. This could have led to malicious websites storing tracking data without permission. This vulnerability affects Firefox < 115. **CVE ID : CVE-2023-3482**	https://www.mozilla.org/security/advisories/mfsa2023-22/	A-MOZ-FIRE-240723/378
N/A	05-Jul-2023	6.5	A website could have obscured the fullscreen notification by using an option element by introducing lag via an expensive computational function. This could have led to user confusion and	https://www.mozilla.org/security/advisories/mfsa2023-22/	A-MOZ-FIRE-240723/379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible spoofing attacks. This vulnerability affects Firefox < 115. **CVE ID : CVE-2023-37204**		
N/A	05-Jul-2023	6.5	The use of RTL Arabic characters in the address bar may have allowed for URL spoofing. This vulnerability affects Firefox < 115. **CVE ID : CVE-2023-37205**	https://www.mozilla.org/security/advisories/mfsa2023-22/	A-MOZ-FIRE-240723/380
Improper Link Resolution Before File Access ('Link Following')	05-Jul-2023	6.5	Uploading files which contain symlinks may have allowed an attacker to trick a user into submitting sensitive data to a malicious website. This vulnerability affects Firefox < 115. **CVE ID : CVE-2023-37206**	https://www.mozilla.org/security/advisories/mfsa2023-22/	A-MOZ-FIRE-240723/381
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	05-Jul-2023	6.5	A website could have obscured the fullscreen notification by using a URL with a scheme handled by an external program, such as a mailto URL. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 115, Firefox ESR < 102.13,	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	A-MOZ-FIRE-240723/382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Thunderbird < 102.13. **CVE ID : CVE-2023-37207**		
N/A	05-Jul-2023	6.5	A website could prevent a user from exiting full-screen mode via alert and prompt calls. This could lead to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 115. **CVE ID : CVE-2023-37210**	https://www.mozilla.org/security/advisories/mfsa2023-22/	A-MOZ-FIRE-240723/383
Product: firefox_esr					
Affected Version(s): * Up to (excluding) 102.13					
Use After Free	05-Jul-2023	8.8	An attacker could have triggered a use-after-free condition when creating a WebRTC connection over HTTPS. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37201**	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	A-MOZ-FIRE-240723/384
Use After Free	05-Jul-2023	8.8	Cross-compartment wrappers wrapping a scripted proxy could have caused objects from other compartments to be stored in the main compartment	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/a	A-MOZ-FIRE-240723/385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a use-after-free. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37202**	dvisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	
Out-of-bounds Write	05-Jul-2023	8.8	Memory safety bugs present in Firefox 114, Firefox ESR 102.12, and Thunderbird 102.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37211**	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	A-MOZ-FIRE-240723/386
N/A	05-Jul-2023	7.8	When opening Diagcab files, Firefox did not warn the user that these files may contain malicious code. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13.	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/a	A-MOZ-FIRE-240723/387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37208	dvisories/mfsa2023-24/	
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	05-Jul-2023	6.5	A website could have obscured the fullscreen notification by using a URL with a scheme handled by an external program, such as a mailto URL. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37207**	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	A-MOZ-FIRE-240723/388
Product: thunderbird					
Affected Version(s): * Up to (excluding) 102.13					
Use After Free	05-Jul-2023	8.8	An attacker could have triggered a use-after-free condition when creating a WebRTC connection over HTTPS. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37201**	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	A-MOZ-THUN-240723/389
Use After Free	05-Jul-2023	8.8	Cross-compartment wrappers wrapping a scripted proxy could have caused	https://www.mozilla.org/security/advisories/mf	A-MOZ-THUN-240723/390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			objects from other compartments to be stored in the main compartment resulting in a use-after-free. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37202**	sa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	
Out-of-bounds Write	05-Jul-2023	8.8	Memory safety bugs present in Firefox 114, Firefox ESR 102.12, and Thunderbird 102.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37211**	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	A-MOZ-THUN-240723/391
N/A	05-Jul-2023	7.8	When opening Diagcab files, Firefox did not warn the user that these files may contain malicious code. This vulnerability affects Firefox < 115, Firefox ESR < 102.13,	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mf	A-MOZ-THUN-240723/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Thunderbird < 102.13. **CVE ID : CVE-2023-37208**	sa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	05-Jul-2023	6.5	A website could have obscured the fullscreen notification by using a URL with a scheme handled by an external program, such as a mailto URL. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37207**	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	A-MOZ-THUN-240723/393
Vendor: myeventon					
Product: eventon					
Affected Version(s): * Up to (excluding) 2.1.2					
Missing Authorization	10-Jul-2023	5.3	The EventON WordPress plugin before 2.1.2 lacks authentication and authorization in its eventon_ics_download ajax action, allowing unauthenticated visitors to access private and password protected Events by guessing their numeric id.	N/A	A-MYE-EVEN-240723/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2796		
Vendor: nicdark					
Product: nd_shortcodes					
Affected Version(s): * Up to (excluding) 7.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jul-2023	8.8	The ND Shortcodes WordPress plugin before 7.0 does not validate some shortcode attributes before using them to generate paths passed to include function/s, allowing any authenticated users such as subscriber to perform LFI attacks **CVE ID : CVE-2023-1273**	N/A	A-NIC-ND_S-240723/395
Vendor: Nodejs					
Product: node.js					
Affected Version(s): 16.0.0					
N/A	01-Jul-2023	7.5	The llhttp parser in the http module in Node v20.2.0 does not strictly use the CRLF sequence to delimit HTTP requests. This can lead to HTTP Request Smuggling (HRS). The CR character (without LF) is sufficient to delimit HTTP header fields in the llhttp parser. According to	N/A	A-NOD-NODE-240723/396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RFC7230 section 3, only the CRLF sequence should delimit each header-field. This impacts all Node.js active versions: v16, v18, and, v20 **CVE ID : CVE-2023-30589**		
Affected Version(s): 18.0.0					
N/A	01-Jul-2023	7.5	The llhttp parser in the http module in Node v20.2.0 does not strictly use the CRLF sequence to delimit HTTP requests. This can lead to HTTP Request Smuggling (HRS). The CR character (without LF) is sufficient to delimit HTTP header fields in the llhttp parser. According to RFC7230 section 3, only the CRLF sequence should delimit each header-field. This impacts all Node.js active versions: v16, v18, and, v20 **CVE ID : CVE-2023-30589**	N/A	A-NOD-NODE-240723/397
Affected Version(s): 20.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	01-Jul-2023	7.5	A privilege escalation vulnerability exists in Node.js 20 that allowed loading arbitrary OpenSSL engines when the experimental permission model is enabled, which can bypass and/or disable the permission model. The attack complexity is high. However, the crypto.setEngine() API can be used to bypass the permission model when called with a compatible OpenSSL engine. The OpenSSL engine can, for example, disable the permission model in the host process by manipulating the process's stack memory to locate the permission model Permission::enabled_ in the host process's heap memory. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. **CVE ID : CVE-2023-30586**	N/A	A-NOD-NODE-240723/398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Jul-2023	7.5	The llhttp parser in the http module in Node v20.2.0 does not strictly use the CRLF sequence to delimit HTTP requests. This can lead to HTTP Request Smuggling (HRS). The CR character (without LF) is sufficient to delimit HTTP header fields in the llhttp parser. According to RFC7230 section 3, only the CRLF sequence should delimit each header-field. This impacts all Node.js active versions: v16, v18, and, v20 **CVE ID : CVE-2023-30589**	N/A	A-NOD-NODE-240723/399
Affected Version(s): 20.2.0					
N/A	01-Jul-2023	7.5	The llhttp parser in the http module in Node v20.2.0 does not strictly use the CRLF sequence to delimit HTTP requests. This can lead to HTTP Request Smuggling (HRS).	N/A	A-NOD-NODE-240723/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The CR character (without LF) is sufficient to delimit HTTP header fields in the llhttp parser. According to RFC7230 section 3, only the CRLF sequence should delimit each header-field. This impacts all Node.js active versions: v16, v18, and, v20 **CVE ID : CVE-2023-30589**		
Vendor: novu					
Product: novu					
Affected Version(s): * Up to (excluding) 0.16					
URL Redirection to Untrusted Site ('Open Redirect')	06-Jul-2023	6.1	Novu provides an API for sending notifications through multiple channels. Versions prior to 0.16.0 contain an open redirect vulnerability in the "Sign In with GitHub" functionality of Novu's open-source repository. It could have allowed an attacker to force a victim into opening a malicious URL and thus, potentially log into the repository under the victim's account gaining full control of the account. This	https://github.com/novuhq/novu/security/advisories/GHSA-xxv3-m43w-gv79, https://github.com/novuhq/novu/pull/3510	A-NOV-NOVU-240723/401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability only affected the Novu Cloud and Open-Source deployments if the user manually enabled the GitHub OAuth on their self-hosted instance of Novu. Users should upgrade to version 0.16.0 to receive a patch. **CVE ID : CVE-2023-35948**		
Vendor: Nullsoft					
Product: nullsoft_scriptable_install_system					
Affected Version(s): * Up to (including) 3.09					
N/A	03-Jul-2023	5.3	Nullsoft Scriptable Install System (NSIS) before 3.09 mishandles access control for an uninstaller directory. **CVE ID : CVE-2023-37378**	https://github.com/kichik/nsis/commit/281e2851fe669d10e0650fc89d0e7fb74a598967, https://github.com/kichik/nsis/commit/409b5841479c44fbf33a6ba97c1146e46f965467, https://github.com/kichik/nsis/commit/c40cf78994e74a1a3a381a850c996b251e3277c0	A-NUL-NULL-240723/402
Vendor: Nvidia					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: cuda_toolkit					
Affected Version(s): * Up to (excluding) 12.2					
NULL Pointer Dereference	04-Jul-2023	3.3	NVIDIA CUDA toolkit for Linux and Windows contains a vulnerability in the nvdisasm binary file, where an attacker may cause a NULL pointer dereference by providing a user with a malformed ELF file. A successful exploit of this vulnerability may lead to a partial denial of service. **CVE ID : CVE-2023-25523**	https://nvidia.custhelp.com/app/answers/detail/a_id/5469	A-NVI-CUDA-240723/403
Product: gpu_display_driver					
Affected Version(s): * Up to (excluding) 11.13					
N/A	04-Jul-2023	7.1	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where a guest OS may be able to control resources for which it is not authorized, which	https://nvidia.custhelp.com/app/answers/detail/a_id/5468	A-NVI-GPU_-240723/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may lead to information disclosure and data tampering. **CVE ID : CVE-2023-25517**		
Affected Version(s): * Up to (including) 11.12					
Integer Overflow or Wraparound	04-Jul-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where an unprivileged user can cause an integer overflow, which may lead to information disclosure and denial of service. **CVE ID : CVE-2023-25516**	N/A	A-NVI-GPU_-240723/405
Affected Version(s): From (including) 13.0 Up to (excluding) 13.8					
N/A	04-Jul-2023	7.1	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where a guest OS may be able to control resources for which it is not authorized, which may lead to information	https://nvidia.custhelp.com/app/answers/detail/a_id/5468	A-NVI-GPU_-240723/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure and data tampering. **CVE ID : CVE-2023-25517**		
Affected Version(s): From (including) 13.0 Up to (including) 13.7					
Integer Overflow or Wraparound	04-Jul-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where an unprivileged user can cause an integer overflow, which may lead to information disclosure and denial of service. **CVE ID : CVE-2023-25516**	N/A	A-NVI-GPU_-240723/407
Affected Version(s): From (including) 15.0 Up to (excluding) 15.3					
N/A	04-Jul-2023	7.1	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where a guest OS may be able to control resources for which it is not authorized, which may lead to information disclosure and data tampering.	https://nvidia.custhelp.com/app/answers/detail/a_id/5468	A-NVI-GPU_-240723/408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25517		
Affected Version(s): From (including) 15.0 Up to (including) 15.2					
Integer Overflow or Wraparound	04-Jul-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where an unprivileged user can cause an integer overflow, which may lead to information disclosure and denial of service. **CVE ID : CVE-2023-25516**	N/A	A-NVI-GPU_-240723/409
Vendor: o					
Product: milesight					
Affected Version(s): milesightvpn					
Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	06-Jul-2023	4.7	Cross-site scripting (xss) vulnerabilities exist in the requestHandlers.js detail_device functionality of Milesight VPN v2.0.2. A specially-crafted HTTP request can lead to arbitrary Javascript code injection. An attacker can send an HTTP request to trigger these	N/A	A-O-MILE-240723/410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities.This XSS is exploited through the remote_subnet field of the database **CVE ID : CVE-2023-24497**		
Vendor: onesttech					
Product: onest_customer_relation_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jul-2023	6.1	A vulnerability was found in Onest CRM 1.0. It has been classified as problematic. This affects an unknown part of the file /admin/project/update/2 of the component Project List Handler. The manipulation of the argument name with the input <script>alert(1)</script> leads to cross site scripting. It is possible to initiate the attack remotely. The identifier VDB-232953 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3505**	N/A	A-ONE-ONES-240723/411
Vendor: online_examination_system_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: online_examination_system					
Affected Version(s): 1.0					
Cross-Site Request Forgery (CSRF)	07-Jul-2023	6.5	The Online Examination System Project 1.0 version is vulnerable to Cross-Site Request Forgery (CSRF) attacks. An attacker can craft a malicious link that, when clicked by an admin user, will delete a user account from the database without the admin's consent. The email of the user to be deleted is passed as a parameter in the URL, which can be manipulated by the attacker. This could result in a loss of data. **CVE ID : CVE-2023-36256**	N/A	A-ONL-ONLI-240723/412
Vendor: online_pizza_ordering_system_project					
Product: online_pizza_ordering_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	10-Jul-2023	9.8	Sourcecodester Online Pizza Ordering System v1.0 allows the upload of malicious PHP files resulting in Remote Code Execution (RCE). **CVE ID : CVE-2023-37151**	N/A	A-ONL-ONLI-240723/413
Improper Neutralizat	10-Jul-2023	6.1	Sourcecodester Online Pizza	N/A	A-ONL-ONLI-240723/414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Ordering System v1.0 has a Cross-site scripting (XSS) vulnerability in "/admin/index.php?page=categories" Category item. **CVE ID : CVE-2023-37150**		
Vendor: oopspam					
Product: oopspam_anti-spam					
Affected Version(s): * Up to (excluding) 1.1.45					
Cross-Site Request Forgery (CSRF)	11-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in OOPSpam OOPSpam Anti-Spam plugin <= 1.1.44 versions. **CVE ID : CVE-2023-35913**	N/A	A-OOP-OOPS-240723/415
Vendor: openimageio					
Product: openimageio					
Affected Version(s): * Up to (including) 2.4.12.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Jul-2023	7.8	Buffer Overflow vulnerability in OpenImageIO v.2.4.12.0 and before allows a remote to execute arbitrary code and obtain sensitive information via a crafted file to the readimg function. **CVE ID : CVE-2023-36183**	https://github.com/OpenImageIO/oiio/issues/3871	A-OPE-OPEN-240723/416
Vendor: osslsigncode_project					
Product: osslsigncode					
Affected Version(s): 2.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Jul-2023	7.8	Buffer Overflow vulnerability in mtrojnar osslsigncode v.2.3 and before allows a local attacker to execute arbitrary code via a crafted .exe, .sys, and .dll files. **CVE ID : CVE-2023-36377**	N/A	A-OSS-OSSL-240723/417
Vendor: ozette					
Product: simple_mobile_url_redirect					
Affected Version(s): * Up to (including) 1.7.2					
Cross-Site Request Forgery (CSRF)	10-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Ozette Plugins Simple Mobile URL Redirect plugin <= 1.7.2 versions. **CVE ID : CVE-2023-23897**	N/A	A-OZE-SIMP-240723/418
Vendor: pandoc					
Product: pandoc					
Affected Version(s): From (including) 1.13 Up to (excluding) 3.1.4					
N/A	05-Jul-2023	5	Pandoc is a Haskell library for converting from one markup format to another, and a command-line tool that uses this library. Starting in version 1.13 and prior to version 3.1.4, Pandoc is susceptible to an arbitrary file write vulnerability, which can be triggered by	https://github.com/jgm/pandoc/security/advisories/GHSA-xj5q-fv23-575g	A-PAN-PAND-240723/419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			providing a specially crafted image element in the input when generating files using the `--extract-media` option or outputting to PDF format. This vulnerability allows an attacker to create or overwrite arbitrary files on the system ,depending on the privileges of the process running pandoc. It only affects systems that pass untrusted user input to pandoc and allow pandoc to be used to produce a PDF or with the `--extract-media` option. The fix is to unescape the percent-encoding prior to checking that the resource is not above the working directory, and prior to extracting the extension. Some code for checking that the path is below the working directory was flawed in a similar way and has also been fixed. Note that the `--sandbox` option,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which only affects IO done by readers and writers themselves, does not block this vulnerability. The vulnerability is patched in pandoc 3.1.4. As a workaround, audit the pandoc command and disallow PDF output and the `--extract-media` option. **CVE ID : CVE-2023-35936**		
Vendor: Piwigo					
Product: piwigo					
Affected Version(s): * Up to (excluding) 13.8.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jul-2023	8.8	Piwigo is open source photo gallery software. Prior to version 13.8.0, there is a SQL Injection vulnerability in the login of the administrator screen. The SQL statement that acquires the HTTP Header `User-Agent` is vulnerable at the endpoint that records user information when logging in to the administrator screen. It is possible to execute arbitrary SQL statements. Someone who wants	https://github.com/Piwigo/Piwigo/commit/978425527d6c113887f845d75cf982bbb62d761a	A-PIW-PIWI-240723/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to exploit the vulnerability must be log in to the administrator screen, even with low privileges. Any SQL statement can be executed. Doing so may leak information from the database. Version 13.8.0 contains a fix for this issue. As another mitigation, those who want to execute a SQL statement verbatim with user-enterable parameters should be sure to escape the parameter contents appropriately. **CVE ID : CVE-2023-37270**		
Vendor: pixelgrade					
Product: comments_rating					
Affected Version(s): * Up to (excluding) 1.1.7					
Cross-Site Request Forgery (CSRF)	11-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Pixelgrade Comments Ratings plugin <= 1.1.6 versions. **CVE ID : CVE-2023-23704**	N/A	A-PIX-COMM-240723/421
Product: pixtypes					
Affected Version(s): * Up to (excluding) 1.4.15					
Cross-Site Request	11-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in	N/A	A-PIX-PIXT-240723/422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			Pixelgrade PixTypes plugin <= 1.4.14 versions. **CVE ID : CVE-2023-25487**		
Vendor: premmerce					
Product: redirect_manager					
Affected Version(s): * Up to (including) 1.0.9					
Cross-Site Request Forgery (CSRF)	10-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Premmerce Premmerce Redirect Manager plugin <= 1.0.9 versions. **CVE ID : CVE-2023-23787**	N/A	A-PRE-REDI-240723/423
Vendor: Progress					
Product: moveit_transfer					
Affected Version(s): * Up to (excluding) 12.1.11					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2023	9.1	In Progress MOVEit Transfer before 2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), a SQL injection vulnerability has been identified in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could	https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023	A-PRO-MOVE-240723/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			submit a crafted payload to a MOVEit Transfer application endpoint that could result in modification and disclosure of MOVEit database content. **CVE ID : CVE-2023-36934**		
Affected Version(s): * Up to (excluding) 2020.1.11					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2023	8.1	In Progress MOVEit Transfer before 2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), multiple SQL injection vulnerabilities have been identified in the MOVEit Transfer web application that could allow an authenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted payload to a MOVEit Transfer application endpoint that could result in modification and disclosure of MOVEit database content. **CVE ID : CVE-2023-36932**	https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023	A-PRO-MOVE-240723/425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	05-Jul-2023	7.5	In Progress MOVEit Transfer before 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), it is possible for an attacker to invoke a method that results in an unhandled exception. Triggering this workflow can cause the MOVEit Transfer application to terminate unexpectedly. **CVE ID : CVE-2023-36933**	https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023	A-PRO-MOVE-240723/426
Affected Version(s): From (including) 13.0.0 Up to (excluding) 13.0.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2023	9.1	In Progress MOVEit Transfer before 2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), a SQL injection vulnerability has been identified in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted	https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023	A-PRO-MOVE-240723/427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload to a MOVEit Transfer application endpoint that could result in modification and disclosure of MOVEit database content. **CVE ID : CVE-2023-36934**		
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2023	9.1	In Progress MOVEit Transfer before 2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), a SQL injection vulnerability has been identified in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted payload to a MOVEit Transfer application endpoint that could result in modification and disclosure of MOVEit database content. **CVE ID : CVE-2023-36934**	https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023	A-PRO-MOVE-240723/428
Affected Version(s): From (including) 14.0.0 Up to (excluding) 14.0.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2023	9.1	In Progress MOVEit Transfer before 2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), a SQL injection vulnerability has been identified in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted payload to a MOVEit Transfer application endpoint that could result in modification and disclosure of MOVEit database content. **CVE ID : CVE-2023-36934**	https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023	A-PRO-MOVE-240723/429
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2023	9.1	In Progress MOVEit Transfer before 2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), a SQL injection vulnerability has	https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023	A-PRO-MOVE-240723/430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been identified in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted payload to a MOVEit Transfer application endpoint that could result in modification and disclosure of MOVEit database content. **CVE ID : CVE-2023-36934**		
Affected Version(s): From (including) 15.0.0 Up to (excluding) 15.0.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2023	9.1	In Progress MOVEit Transfer before 2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), a SQL injection vulnerability has been identified in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted	https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023	A-PRO-MOVE-240723/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload to a MOVEit Transfer application endpoint that could result in modification and disclosure of MOVEit database content. **CVE ID : CVE-2023-36934**		
Affected Version(s): From (including) 2021.0 Up to (excluding) 2021.0.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2023	8.1	In Progress MOVEit Transfer before 2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), multiple SQL injection vulnerabilities have been identified in the MOVEit Transfer web application that could allow an authenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted payload to a MOVEit Transfer application endpoint that could result in modification and disclosure of MOVEit database content. **CVE ID : CVE-2023-36932**	https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023	A-PRO-MOVE-240723/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	05-Jul-2023	7.5	In Progress MOVEit Transfer before 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), it is possible for an attacker to invoke a method that results in an unhandled exception. Triggering this workflow can cause the MOVEit Transfer application to terminate unexpectedly. **CVE ID : CVE-2023-36933**	https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023	A-PRO-MOVE-240723/433
Affected Version(s): From (including) 2021.1.0 Up to (excluding) 2021.1.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2023	8.1	In Progress MOVEit Transfer before 2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), multiple SQL injection vulnerabilities have been identified in the MOVEit Transfer web application that could allow an authenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted	https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023	A-PRO-MOVE-240723/434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload to a MOVEit Transfer application endpoint that could result in modification and disclosure of MOVEit database content. **CVE ID : CVE-2023-36932**		
Improper Handling of Exceptional Conditions	05-Jul-2023	7.5	In Progress MOVEit Transfer before 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), it is possible for an attacker to invoke a method that results in an unhandled exception. Triggering this workflow can cause the MOVEit Transfer application to terminate unexpectedly. **CVE ID : CVE-2023-36933**	https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023	A-PRO-MOVE-240723/435
Affected Version(s): From (including) 2022.0.0 Up to (excluding) 2022.0.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2023	8.1	In Progress MOVEit Transfer before 2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), multiple SQL injection vulnerabilities have been identified in the	https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023	A-PRO-MOVE-240723/436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOVEit Transfer web application that could allow an authenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted payload to a MOVEit Transfer application endpoint that could result in modification and disclosure of MOVEit database content. **CVE ID : CVE-2023-36932**		
Improper Handling of Exceptional Conditions	05-Jul-2023	7.5	In Progress MOVEit Transfer before 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), it is possible for an attacker to invoke a method that results in an unhandled exception. Triggering this workflow can cause the MOVEit Transfer application to terminate unexpectedly. **CVE ID : CVE-2023-36933**	https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023	A-PRO-MOVE-240723/437
Affected Version(s): From (including) 2022.1.0 Up to (excluding) 2022.1.8					
Improper Neutralizat	05-Jul-2023	8.1	In Progress MOVEit Transfer before	https://community.prog	A-PRO-MOVE-240723/438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), multiple SQL injection vulnerabilities have been identified in the MOVEit Transfer web application that could allow an authenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted payload to a MOVEit Transfer application endpoint that could result in modification and disclosure of MOVEit database content. **CVE ID : CVE-2023-36932**	ress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023	
Improper Handling of Exceptional Conditions	05-Jul-2023	7.5	In Progress MOVEit Transfer before 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), it is possible for an attacker to invoke a method that results in an unhandled exception. Triggering this workflow can	https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023	A-PRO-MOVE-240723/439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause the MOVEit Transfer application to terminate unexpectedly. **CVE ID : CVE-2023-36933**		
Affected Version(s): From (including) 2023.0.0 Up to (excluding) 2023.0.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jul-2023	8.1	In Progress MOVEit Transfer before 2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), multiple SQL injection vulnerabilities have been identified in the MOVEit Transfer web application that could allow an authenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted payload to a MOVEit Transfer application endpoint that could result in modification and disclosure of MOVEit database content. **CVE ID : CVE-2023-36932**	https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023	A-PRO-MOVE-240723/440
Improper Handling of Exceptiona	05-Jul-2023	7.5	In Progress MOVEit Transfer before 2021.0.9 (13.0.9), 2021.1.7 (13.1.7),	https://community.progress.com/s/article/MOVEi	A-PRO-MOVE-240723/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), it is possible for an attacker to invoke a method that results in an unhandled exception. Triggering this workflow can cause the MOVEit Transfer application to terminate unexpectedly. **CVE ID : CVE-2023-36933**	t-Transfer-2020-1-Service-Pack-July-2023	
Vendor: protobufjs_project					
Product: protobufjs					
Affected Version(s): From (including) 6.10.0 Up to (excluding) 7.2.4					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	05-Jul-2023	9.8	protobuf.js (aka protobufjs) 6.10.0 through 7.x before 7.2.4 allows Prototype Pollution, a different vulnerability than CVE-2022-25878. A user-controlled protobuf message can be used by an attacker to pollute the prototype of Object.prototype by adding and overwriting its data and functions. Exploitation can involve: (1) using the function parse to parse protobuf messages on the fly, (2) loading .proto	https://github.com/protobufjs/protobuf.js/commit/e66379f451b0393c27d87b37fa7d271619e16b0d, https://github.com/protobufjs/protobuf.js/compare/protobufjs-v7.2.3...protobufjs-v7.2.4, https://github.com/protobufjs/protobuf.js/pull/1899	A-PRO-PROT-240723/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files by using load/loadSync functions, or (3) providing untrusted input to the functions ReflectionObject.setParsedOption and util.setProperty. NOTE: this CVE Record is about "Object.constructor.prototype.<new-property> = ...;" whereas CVE-2022-25878 was about "Object.__proto__.<new-property> = ...;" instead. **CVE ID : CVE-2023-36665**		
Vendor: pvmg					
Product: reservation.studio					
Affected Version(s): * Up to (including) 1.0.11					
Cross-Site Request Forgery (CSRF)	11-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Reservation.Studio Reservation.Studio widget plugin <= 1.0.11 versions. **CVE ID : CVE-2023-25468**	N/A	A-PVM-RESE-240723/443
Vendor: Redhat					
Product: build_of_quarkus					
Affected Version(s): * Up to (excluding) 2.13.8					
N/A	04-Jul-2023	8.1	A vulnerability was found in quarkus-core. This vulnerability occurs because the TLS	https://bugzilla.redhat.com/show_bug.cgi?id=2211026,	A-RED-BUIL-240723/444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protocol configured with quarkus.http.ssl.protocols is not enforced, and the client can force the selection of the weaker supported TLS protocol. **CVE ID : CVE-2023-2974**	https://access.redhat.com/security/cve/CVE-2023-2974	
Product: openshift					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	10-Jul-2023	7.5	IBM Watson CP4D Data Stores 4.6.0 does not properly allocate resources without limits or throttling which could allow a remote attacker with information specific to the system to cause a denial of service. IBM X-Force ID: 248924. **CVE ID : CVE-2023-27540**	https://www.ibm.com/support/pages/node/7009883, https://exchange.xforce.ibmcloud.com/vulnerabilities/248924	A-RED-OPEN-240723/445
Product: openshift_container_platform					
Affected Version(s): 4.10					
Weak Password Requirements	05-Jul-2023	7.5	A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat discovered that, when FIPS mode was enabled, not all of the cryptographic modules in use were FIPS-validated.	https://access.redhat.com/security/cve/CVE-2023-3089, https://bugzilla.redhat.com/show_bug.cgi?id=2212085	A-RED-OPEN-240723/446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3089		
Product: openshift_container_platform_for_arm64					
Affected Version(s): 4.10					
Weak Password Requirements	05-Jul-2023	7.5	A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat discovered that, when FIPS mode was enabled, not all of the cryptographic modules in use were FIPS-validated. **CVE ID : CVE-2023-3089**	https://access.redhat.com/security/cve/CVE-2023-3089, https://bugzilla.redhat.com/show_bug.cgi?id=2212085	A-RED-OPEN-240723/447
Affected Version(s): 4.11					
Weak Password Requirements	05-Jul-2023	7.5	A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat discovered that, when FIPS mode was enabled, not all of the cryptographic modules in use were FIPS-validated. **CVE ID : CVE-2023-3089**	https://access.redhat.com/security/cve/CVE-2023-3089, https://bugzilla.redhat.com/show_bug.cgi?id=2212085	A-RED-OPEN-240723/448
Affected Version(s): 4.12					
Weak Password Requirements	05-Jul-2023	7.5	A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat discovered that, when FIPS mode was enabled, not all of the cryptographic	https://access.redhat.com/security/cve/CVE-2023-3089, https://bugzilla.redhat.com/show_bug	A-RED-OPEN-240723/449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modules in use were FIPS-validated. **CVE ID : CVE-2023-3089**	.cgi?id=2212085	
Product: openshift_container_platform_for_linuxone					
Affected Version(s): 4.10					
Weak Password Requirements	05-Jul-2023	7.5	A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat discovered that, when FIPS mode was enabled, not all of the cryptographic modules in use were FIPS-validated. **CVE ID : CVE-2023-3089**	https://access.redhat.com/security/cve/CVE-2023-3089, https://bugzilla.redhat.com/show_bug.cgi?id=2212085	A-RED-OPEN-240723/450
Affected Version(s): 4.11					
Weak Password Requirements	05-Jul-2023	7.5	A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat discovered that, when FIPS mode was enabled, not all of the cryptographic modules in use were FIPS-validated. **CVE ID : CVE-2023-3089**	https://access.redhat.com/security/cve/CVE-2023-3089, https://bugzilla.redhat.com/show_bug.cgi?id=2212085	A-RED-OPEN-240723/451
Affected Version(s): 4.12					
Weak Password Requirements	05-Jul-2023	7.5	A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat discovered that, when FIPS mode was	https://access.redhat.com/security/cve/CVE-2023-3089, https://bugzilla.redhat.co	A-RED-OPEN-240723/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabled, not all of the cryptographic modules in use were FIPS-validated. **CVE ID : CVE-2023-3089**	m/show_bug.cgi?id=2212085	
Product: openshift_container_platform_for_power					
Affected Version(s): 4.10					
Weak Password Requirements	05-Jul-2023	7.5	A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat discovered that, when FIPS mode was enabled, not all of the cryptographic modules in use were FIPS-validated. **CVE ID : CVE-2023-3089**	https://access.redhat.com/security/cve/CVE-2023-3089, https://bugzilla.redhat.com/show_bug.cgi?id=2212085	A-RED-OPEN-240723/453
Affected Version(s): 4.11					
Weak Password Requirements	05-Jul-2023	7.5	A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat discovered that, when FIPS mode was enabled, not all of the cryptographic modules in use were FIPS-validated. **CVE ID : CVE-2023-3089**	https://access.redhat.com/security/cve/CVE-2023-3089, https://bugzilla.redhat.com/show_bug.cgi?id=2212085	A-RED-OPEN-240723/454
Affected Version(s): 4.12					
Weak Password Requirements	05-Jul-2023	7.5	A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat	https://access.redhat.com/security/cve/CVE-2023-3089,	A-RED-OPEN-240723/455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered that, when FIPS mode was enabled, not all of the cryptographic modules in use were FIPS-validated. **CVE ID : CVE-2023-3089**	https://bugzilla.redhat.com/show_bug.cgi?id=2212085	
Product: openshift_container_platform_ibm_z_systems					
Affected Version(s): 4.10					
Weak Password Requirements	05-Jul-2023	7.5	A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat discovered that, when FIPS mode was enabled, not all of the cryptographic modules in use were FIPS-validated. **CVE ID : CVE-2023-3089**	https://access.redhat.com/security/cve/CVE-2023-3089, https://bugzilla.redhat.com/show_bug.cgi?id=2212085	A-RED-OPEN-240723/456
Affected Version(s): 4.11					
Weak Password Requirements	05-Jul-2023	7.5	A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat discovered that, when FIPS mode was enabled, not all of the cryptographic modules in use were FIPS-validated. **CVE ID : CVE-2023-3089**	https://access.redhat.com/security/cve/CVE-2023-3089, https://bugzilla.redhat.com/show_bug.cgi?id=2212085	A-RED-OPEN-240723/457
Affected Version(s): 4.12					
Weak Password	05-Jul-2023	7.5	A compliance problem was found in the Red Hat	https://access.redhat.com/security/	A-RED-OPEN-240723/458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Requirements			OpenShift Container Platform. Red Hat discovered that, when FIPS mode was enabled, not all of the cryptographic modules in use were FIPS-validated. **CVE ID : CVE-2023-3089**	cve/CVE-2023-3089, https://bugzilla.redhat.com/show_bug.cgi?id=2212085	
Vendor: rotem-dynamics					
Product: rotem_crm					
Affected Version(s): * Up to (including) 2023-07-29					
Observable Discrepancy	06-Jul-2023	7.5	A vulnerability classified as problematic has been found in Rotem Dynamics Rotem CRM up to 20230729. This affects an unknown part of the file /LandingPages/api/otp/send?id=[ID][ampersand]method=sms of the component OTP URI Interface. The manipulation leads to information exposure through discrepancy. It is possible to initiate the attack remotely. The identifier VDB-233253 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	A-ROT-ROTE-240723/459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3529		
Vendor: rsvpmaker_project					
Product: rsvpmaker					
Affected Version(s): * Up to (excluding) 10.5.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Jul-2023	7.2	Auth. (admin+) SQL Injection (SQLi) vulnerability in David F. Carr RSVPMaker plugin < 10.5.5 versions. **CVE ID : CVE-2023-29095**	N/A	A-RSV-RSVP-240723/460
Vendor: salesforce					
Product: tough-cookie					
Affected Version(s): * Up to (excluding) 4.1.3					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	01-Jul-2023	9.8	Versions of the package tough-cookie before 4.1.3 are vulnerable to Prototype Pollution due to improper handling of Cookies when using CookieJar in rejectPublicSuffixes=false mode. This issue arises from the manner in which the objects are initialized. **CVE ID : CVE-2023-26136**	https://github.com/salesforce/tough-cookie/issues/282, https://github.com/salesforce/tough-cookie/commit/12d474791bb856004e858fdb1c47b7608d09cf6e	A-SAL-TOUG-240723/461
Vendor: Samsung					
Product: calendar					
Affected Version(s): * Up to (excluding) 12.4.07.15					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jul-2023	5.5	Potential zip path traversal vulnerability in Calendar application prior to version 12.4.07.15 in Android 13 allows attackers to write arbitrary file. **CVE ID : CVE-2023-30678**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=07	A-SAM-CALE-240723/462
Product: internet					
Affected Version(s): * Up to (excluding) 21.0.0.41					
N/A	06-Jul-2023	6.5	Improper configuration in Samsung Internet prior to version 21.0.0.41 allows attacker to bypass SameSite Cookie. **CVE ID : CVE-2023-30674**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=07	A-SAM-INTE-240723/463
Product: pass					
Affected Version(s): * Up to (excluding) 4.2.03.1					
Improper Authentication	06-Jul-2023	5.5	Improper authentication in Samsung Pass prior to version 4.2.03.1 allows local attacker to access stored account information when Samsung Wallet is not installed. **CVE ID : CVE-2023-30675**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=07	A-SAM-PASS-240723/464
N/A	06-Jul-2023	4.6	Improper access control vulnerability in Samsung Pass prior to version 4.2.03.1 allows	https://security.samsungmobile.com/serviceWeb.smsb?year=2	A-SAM-PASS-240723/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			physical attackers to access data of Samsung Pass. **CVE ID : CVE-2023-30676**	023&month=07	
N/A	06-Jul-2023	4.6	Improper access control vulnerability in Samsung Pass prior to version 4.2.03.1 allows physical attackers to access data of Samsung Pass on a certain state of an unlocked device. **CVE ID : CVE-2023-30677**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=07	A-SAM-PASS-240723/466
Product: smart_switch_pc					
Affected Version(s): * Up to (excluding) 4.3.23043_3					
N/A	06-Jul-2023	5.5	Improper privilege management vulnerability in Samsung Smart Switch for Windows Installer prior to version 4.3.23043_3 allows attackers to cause permanent DoS via directory junction. **CVE ID : CVE-2023-30672**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=07	A-SAM-SMAR-240723/467
Affected Version(s): * Up to (excluding) 4.3.23052_1					
Improper Validation of Integrity Check Value	06-Jul-2023	5.5	Improper validation of integrity check vulnerability in Smart Switch PC prior to version 4.3.23052_1 allows local attackers to delete arbitrary	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=07	A-SAM-SMAR-240723/468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			directory using directory junction. **CVE ID : CVE-2023-30673**		
Vendor: sanitize_project					
Product: sanitize					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 6.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2023	6.1	Sanitize is an allowlist-based HTML and CSS sanitizer. Using carefully crafted input, an attacker may be able to sneak arbitrary HTML and CSS through Sanitize starting with version 3.0.0 and prior to version 6.0.2 when Sanitize is configured to use the built-in "relaxed" config or when using a custom config that allows `style` elements and one or more CSS at-rules. This could result in cross-site scripting or other undesired behavior when the malicious HTML and CSS are rendered in a browser. Sanitize 6.0.2 performs additional escaping of CSS in `style` element content, which fixes this issue. Users who are unable to upgrade can prevent this	https://github.com/rgrove/sanitize/security/advisories/GHSA-f5ww-cq3m-q3g7, https://github.com/rgrove/sanitize/commit/76ed46e6dc70820f38efe27de8dabd54dddb5220	A-SAN-SANI-240723/469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue by using a Sanitize config that doesn't allow `style` elements, using a Sanitize config that doesn't allow CSS at-rules, or by manually escaping the character sequence `</` as `<\/` in `style` element content. **CVE ID : CVE-2023-36823**		
Vendor: scipy					
Product: scipy					
Affected Version(s): * Up to (excluding) 1.11.1					
N/A	05-Jul-2023	5.5	A refcounting issue which leads to potential memory leak was discovered in scipy commit 8627df31ab in Py_FindObjects() function. **CVE ID : CVE-2023-25399**	https://github.com/scipy/scipy/issues/16235, https://github.com/scipy/scipy/pull/16397	A-SCI-SCIP-240723/470
Vendor: seacms					
Product: seacms					
Affected Version(s): 12.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Site Setup module of SEACMS v12.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload. **CVE ID : CVE-2023-37124**	N/A	A-SEA-SEAC-240723/471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Management Custom label module of SEACMS v12.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload. **CVE ID : CVE-2023-37125**	N/A	A-SEA-SEAC-240723/472
Vendor: servicenow					
Product: servicenow					
Affected Version(s): san_diego					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2023	6.1	ServiceNow has released upgrades and patches that address a Reflected Cross-Site scripting (XSS) vulnerability that was identified in the ServiceNow Polaris Layout. This vulnerability would enable an authenticated user to inject arbitrary scripts. **CVE ID : CVE-2023-1298**	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1310230	A-SER-SERV-240723/473
Affected Version(s): tokyo					
Improper Neutralization of Input During Web Page Generation	06-Jul-2023	6.1	ServiceNow has released upgrades and patches that address a Reflected Cross-Site scripting (XSS) vulnerability that was identified in the ServiceNow	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1310230	A-SER-SERV-240723/474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Polaris Layout. This vulnerability would enable an authenticated user to inject arbitrary scripts. **CVE ID : CVE-2023-1298**		
Affected Version(s): utah					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2023	6.1	ServiceNow has released upgrades and patches that address a Reflected Cross-Site scripting (XSS) vulnerability that was identified in the ServiceNow Polaris Layout. This vulnerability would enable an authenticated user to inject arbitrary scripts. **CVE ID : CVE-2023-1298**	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1310230	A-SER-SERV-240723/475
Vendor: shopping_website_project					
Product: shopping_website					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	04-Jul-2023	8.8	A vulnerability has been found in SourceCodester Shopping Website 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file insert-product.php. The	N/A	A-SHO-SHOP-240723/476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation leads to unrestricted upload. 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-232951. **CVE ID : CVE-2023-3503**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jul-2023	7.5	A vulnerability, which was classified as critical, was found in SourceCodester Shopping Website 1.0. Affected is an unknown function of the file search-result.php. The manipulation of the argument product leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-232950 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3502**	N/A	A-SHO-SHOP-240723/477
Improper Neutralization of Special Elements used in an SQL	07-Jul-2023	7.5	A vulnerability was found in SourceCodester Shopping Website 1.0. It has been classified as critical. Affected is an	N/A	A-SHO-SHOP-240723/478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			unknown function of the file check_availability.php. The manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-233286 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3534**		
Vendor: simplephpscripts					
Product: faq_script_php					
Affected Version(s): 2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	6.1	A vulnerability was found in SimplePHPscripts FAQ Script PHP 2.3. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /preview.php of the component URL Parameter Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-233287.	N/A	A-SIM-FAQ_-240723/479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3535		
Product: funeral_script_php					
Affected Version(s): 3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	6.1	A vulnerability was found in SimplePHPscripts Funeral Script PHP 3.1. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /preview.php of the component URL Parameter Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-233288. **CVE ID : CVE-2023-3536**	N/A	A-SIM-FUNE-240723/480
Product: newsletter_script_php					
Affected Version(s): 2.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	6.1	A vulnerability, which was classified as problematic, was found in SimplePHPscripts NewsLetter Script PHP 2.4. Affected is an unknown function of the file /preview.php of the component URL Parameter Handler. The manipulation leads to cross site	N/A	A-SIM-NEWS-240723/481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-233292. **CVE ID : CVE-2023-3540**		
Product: news_script_php_pro					
Affected Version(s): 2.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	6.1	A vulnerability classified as problematic has been found in SimplePHPscripts News Script PHP Pro 2.4. This affects an unknown part of the file /preview.php of the component URL Parameter Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The identifier VDB-233289 was assigned to this vulnerability. **CVE ID : CVE-2023-3537**	N/A	A-SIM-NEWS-240723/482
Product: photo_gallery_php					
Affected Version(s): 2.0					
Improper Neutralization of Input During Web Page Generation	07-Jul-2023	5.4	A vulnerability classified as problematic was found in SimplePHPscripts Photo Gallery PHP 2.0. This	N/A	A-SIM-PHOT-240723/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerability affects unknown code of the file /preview.php of the component URL Parameter Handler. The manipulation leads to cross site scripting. The attack can be initiated remotely. VDB-233290 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3538**		
Product: simple_forum_php					
Affected Version(s): 2.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	6.1	A vulnerability, which was classified as problematic, has been found in SimplePHPscripts Simple Forum PHP 2.7. This issue affects some unknown processing of the file /preview.php of the component URL Parameter Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-233291. **CVE ID : CVE-2023-3539**	N/A	A-SIM-SIMP-240723/484
Vendor: simple_iframe_project					
Product: simple_iframe					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	5.4	The Simple Iframe WordPress plugin before 1.2.0 does not properly validate one of its WordPress block attribute's content, which may allow users whose role is at least that of a contributor to conduct Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-2964**	N/A	A-SIM-SIMP-240723/485
Vendor: smartsoft					
Product: smartbpm.net					
Affected Version(s): 6.70					
Use of Hard-coded Credentials	10-Jul-2023	9.8	SmartSoft SmartBPM.NET has a vulnerability of using hard-coded machine key. An unauthenticated remote attacker can use the machine key to send serialized payload to the server to execute arbitrary code and disrupt service. **CVE ID : CVE-2023-37286**	https://www.twcert.org.tw/tw/cp-132-7221-438c6-1.html	A-SMA-SMAR-240723/486
Use of Hard-coded Credentials	10-Jul-2023	9.1	SmartBPM.NET has a vulnerability of using hard-coded authentication key. An unauthenticated remote attacker can exploit this	https://www.twcert.org.tw/tw/cp-132-7222-cdfd0-1.html	A-SMA-SMAR-240723/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to access system with regular user privilege to read application data, and execute submission and approval processes. **CVE ID : CVE-2023-37287**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Jul-2023	7.5	SmartBPM.NET component has a vulnerability of path traversal within its file download function. An unauthenticated remote attacker can exploit this vulnerability to access arbitrary system files. **CVE ID : CVE-2023-37288**	https://www.twcert.org.tw/tw/cp-132-7223-af8f8-1.html	A-SMA-SMAR-240723/488
Vendor: smartweb_infotech_job_board_project					
Product: smartweb_infotech_job_board					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	04-Jul-2023	9.8	A vulnerability was found in SmartWeb Infotech Job Board 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /settings/account of the component My Profile Page. The manipulation of the argument filename leads to unrestricted	N/A	A-SMA-SMAR-240723/489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upload. The attack may be launched remotely. The identifier of this vulnerability is VDB-232952. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3504**		
Vendor: softmedyazilim					
Product: selfpatron					
Affected Version(s): * Up to (excluding) 2.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Jul-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Softmed SelfPatron allows SQL Injection.This issue affects SelfPatron : before 2.0. **CVE ID : CVE-2023-2852**	N/A	A-SOF-SELF-240723/490
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Softmed SelfPatron allows Reflected	N/A	A-SOF-SELF-240723/491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XSS.This issue affects SelfPatron : before 2.0. **CVE ID : CVE-2023-2853**		
Vendor: Sophos					
Product: iview					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	Cross Site Scripting (XSS) in Sophos Sophos iView (The EOL was December 31st 2020) in grpname parameter that allows arbitrary script to be executed. **CVE ID : CVE-2023-33335**	N/A	A-SOP-IVIE-240723/492
Vendor: sqlfluff					
Product: sqlfluff					
Affected Version(s): * Up to (excluding) 2.1.2					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Jul-2023	7.8	SQLFluff is a SQL linter. Prior to version 2.1.2, in environments where untrusted users have access to the config files, there is a potential security vulnerability where those users could use the `library_path` config value to allow arbitrary python code to be executed via macros. For many users who use SQLFluff in the	https://github.com/sqlfluff/sqlfluff/security/advisories/GHSA-jqhc-m2j3-fjrx	A-SQL-SQLF-240723/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of an environment where all users already have fairly escalated privileges, this may not be an issue - however in larger user bases, or where SQLFluff is bundled into another tool where developers still wish to give users access to supply their on rule configuration, this may be an issue. The 2.1.2 release offers the ability for the `library_path` argument to be overwritten on the command line by using the `--library-path` option. This overrides any values provided in the config files and effectively prevents this route of attack for users which have access to the config file, but not to the scripts which call the SQLFluff CLI directly. A similar option is provided for the Python API, where users also have a greater ability to further customise or override configuration as		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			necessary. Unless `library_path` is explicitly required, SQLFluff maintainers recommend using the option `--library-path none` when invoking SQLFluff which will disable the `library-path` option entirely regardless of the options set in the configuration file or via inline config directives. As a workaround, limiting access to - or otherwise validating configuration files before they are ingested by SQLFluff will provides a similar effect and does not require upgrade. **CVE ID : CVE-2023-36830**		
Vendor: statamic					
Product: statamic					
Affected Version(s): * Up to (excluding) 4.10.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	5.4	Statamic is a flat-first, Laravel and Git powered content management system. Prior to version 4.10.0, the SVG tag does not sanitize malicious SVG. Therefore, an attacker can exploit this vulnerability to	https://github.com/statamic/cms/pull/8408, https://github.com/statamic/cms/commit/c714893ad92de6e5ede17b501003441af50	A-STA-STAT-240723/494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform cross-site scripting attacks using SVG, even when using the `sanitize` function. Version 4.10.0 contains a patch for this issue. **CVE ID : CVE-2023-36828**	5b30d, https://github.com/statamic/cms/security/advisories/GHSA-6r5g-cq4q-327g	
Vendor: stpetedesign					
Product: call_now_accessibility_button					
Affected Version(s): * Up to (excluding) 1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	4.8	The Call Now Accessibility Button WordPress plugin before 1.1 does not properly sanitize some of its settings, which could allow high-privilege users to perform Stored Cross-Site Scripting (XSS) attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID : CVE-2023-2028**	N/A	A-STP-CALL-240723/495
Vendor: taogogo					
Product: taocms					
Affected Version(s): * Up to (including) 3.0.2					
Improper Neutralization of Input During Web Page	05-Jul-2023	6.1	taocms <=3.0.2 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-34654**	N/A	A-TAO-TAOC-240723/496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')					
Vendor: Teampass					
Product: teampass					
Affected Version(s): * Up to (excluding) 3.0.10					
Exposure of Sensitive Information to an Unauthorized Actor	08-Jul-2023	7.5	Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository nilsteampassnet/teampass prior to 3.0.10. **CVE ID : CVE-2023-3553**	https://huntr.dev/bounties/857f002a-2794-4807-aa5d-2f340de01870, https://github.com/nilsteampassnet/teampass/commit/e9f90b746fdde135da3c7fbe4fa22fe2bd32e66b	A-TEA-TEAM-240723/497
Improper Control of Generation of Code ('Code Injection')	08-Jul-2023	7.2	Code Injection in GitHub repository nilsteampassnet/teampass prior to 3.0.10. **CVE ID : CVE-2023-3551**	https://huntr.dev/bounties/cf8878ff-6cd9-49be-b313-7ac2a94fc7f7, https://github.com/nilsteampassnet/teampass/commit/cc6abc76aa46ed4a27736c1d2f21e432a5d54e6f	A-TEA-TEAM-240723/498
Improper Neutralization of Input	06-Jul-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository nilsteampassnet/tea	https://huntr.dev/bounties/c9f0b3ff-bbc4-4ea1-	A-TEA-TEAM-240723/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			mpass prior to 3.0.10. **CVE ID : CVE-2023-3531**	a59e-8594b48bb414, https://github.com/nilsteampassnet/teampass/commit/cb8ea5ccca61653895bb6881547e463baa50293d	
Improper Encoding or Escaping of Output	08-Jul-2023	5.4	Improper Encoding or Escaping of Output in GitHub repository nilsteampassnet/teampass prior to 3.0.10. **CVE ID : CVE-2023-3552**	https://github.com/nilsteampassnet/teampass/commit/8acb4dacc2d008a4186a4e13cc143e978f113955, https://huntr.dev/bounties/aeb2f43f-0602-4ac6-9685-273e87ff4ded	A-TEA-TEAM-240723/500
Vendor: themeum					
Product: tutor_lms					
Affected Version(s): * Up to (excluding) 2.2.1					
Authorization Bypass Through User-Controlled Key	04-Jul-2023	7.5	The Tutor LMS WordPress plugin before 2.2.1 does not implement adequate permission checks for REST API endpoints, allowing unauthenticated attackers to access information from Lessons that should	N/A	A-THE-TUTO-240723/501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not be publicly available. **CVE ID : CVE-2023-3133**		
Vendor: thephpleague					
Product: oauth2-server					
Affected Version(s): From (including) 8.3.2 Up to (excluding) 8.5.3					
Generation of Error Message Containing Sensitive Information	06-Jul-2023	7.5	league/oauth2-server is an implementation of an OAuth 2.0 authorization server written in PHP. Starting in version 8.3.2 and prior to version 8.5.3, servers that passed their keys to the CryptKey constructor as as string instead of a file path will have had that key included in a LogicException message if they did not provide a valid pass phrase for the key where required. This issue has been patched so that the provided key is no longer exposed in the exception message in the scenario outlined above. Users should upgrade to version 8.5.3 to receive the patch. As a workaround, pass the key as a file instead of a string.	https://github.com/thephpleague/oauth2-server/security/advisories/GHSA-wj7q-gjg8-3cpm, https://github.com/thephpleague/oauth2-server/pull/1353	A-THE-OAUT-240723/502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37260		
Vendor: thinutech					
Product: thinu-cms					
Affected Version(s): 1.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jul-2023	9.8	A vulnerability was found in ThinuTech ThinuCMS 1.5. It has been rated as critical. Affected by this issue is some unknown functionality of the file /category.php. The manipulation of the argument cat_id leads to sql injection. The attack may be launched remotely. The identifier of this vulnerability is VDB-233252. **CVE ID : CVE-2023-3528**	N/A	A-THI-THIN-240723/503
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	6.1	A vulnerability has been found in ThinuTech ThinuCMS 1.5 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /author_posts.php. The manipulation of the argument author with the input g6g12<script>alert(1)</script>o8sdm leads to cross site scripting. The attack	N/A	A-THI-THIN-240723/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can be launched remotely. The identifier VDB-233293 was assigned to this vulnerability. **CVE ID : CVE-2023-3541**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	6.1	A vulnerability was found in ThinuTech ThinuCMS 1.5 and classified as problematic. Affected by this issue is some unknown functionality of the file /contact.php. The manipulation of the argument name/body leads to cross site scripting. The attack may be launched remotely. VDB-233294 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3542**	N/A	A-THI-THIN-240723/505
Vendor: tinymce_custom_styles_project					
Product: tinymce_custom_styles					
Affected Version(s): * Up to (excluding) 1.1.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-2023	4.8	The TinyMCE Custom Styles WordPress plugin before 1.1.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting	N/A	A-TIN-TINY-240723/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID : CVE-2023-2967**		
Vendor: travianz_project					
Product: travianz					
Affected Version(s): * Up to (including) 8.3.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2023	6.1	TravianZ through 8.3.4 allows XSS via the Alliance tag/name, the statistics page, the link preferences, the Admin Logs, or the COOKUSR cookie. **CVE ID : CVE-2023-36995**	N/A	A-TRA-TRAV-240723/507
Affected Version(s): 8.3.3					
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	07-Jul-2023	9.8	The cryptographically insecure random number generator being used in TravianZ 8.3.4 and 8.3.3 in the password reset function allows an attacker to guess the password reset.parameters and to take over accounts. **CVE ID : CVE-2023-36993**	N/A	A-TRA-TRAV-240723/508
Incorrect Authorization	07-Jul-2023	9.8	In TravianZ 8.3.4 and 8.3.3, Incorrect Access Control in the installation script	N/A	A-TRA-TRAV-240723/509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows an attacker to overwrite the server configuration and inject PHP code. **CVE ID : CVE-2023-36994**		
Improper Control of Generation of Code ('Code Injection')	07-Jul-2023	7.2	PHP injection in TravianZ 8.3.4 and 8.3.3 in the config editor in the admin page allows remote attackers to execute PHP code. **CVE ID : CVE-2023-36992**	N/A	A-TRA-TRAV-240723/510
Affected Version(s): 8.3.4					
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	07-Jul-2023	9.8	The cryptographically insecure random number generator being used in TravianZ 8.3.4 and 8.3.3 in the password reset function allows an attacker to guess the password reset.parameters and to take over accounts. **CVE ID : CVE-2023-36993**	N/A	A-TRA-TRAV-240723/511
Incorrect Authorization	07-Jul-2023	9.8	In TravianZ 8.3.4 and 8.3.3, Incorrect Access Control in the installation script allows an attacker to overwrite the server configuration and inject PHP code. **CVE ID : CVE-2023-36994**	N/A	A-TRA-TRAV-240723/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	07-Jul-2023	7.2	PHP injection in TravianZ 8.3.4 and 8.3.3 in the config editor in the admin page allows remote attackers to execute PHP code. **CVE ID : CVE-2023-36992**	N/A	A-TRA-TRAV-240723/513
Vendor: trellix					
Product: enterprise_security_manager					
Affected Version(s): * Up to (excluding) 11.6.7					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Jul-2023	8.8	A vulnerability arises out of a failure to comprehensively sanitize the processing of a zip file(s). Incomplete neutralization of external commands used to control the process execution of the .zip application allows an authorized user to obtain control of the .zip application to execute arbitrary commands or obtain elevation of system privileges. **CVE ID : CVE-2023-3314**	https://kcm.trellix.com/corporate/index?page=content&id=SB10403	A-TRE-ENTE-240723/514
Improper Neutralization of Special Elements	03-Jul-2023	7.8	An OS common injection vulnerability exists	https://kcm.trellix.com/corporate/index?page=con	A-TRE-ENTE-240723/515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			in the ESM certificate API, whereby incorrectly neutralized special elements may have allowed an unauthorized user to execute system command injection for the purpose of privilege escalation or to execute arbitrary commands. **CVE ID : CVE-2023-3313**	tent&id=SB10403	
Product: move					
Affected Version(s): * Up to (including) 4.10.0					
Unquoted Search Path or Element	03-Jul-2023	7.8	An unquoted Windows search path vulnerability existed in the install the MOVE 4.10.x and earlier Windows install service (mvagtsce.exe). The misconfiguration allowed an unauthorized local user to insert arbitrary code into the unquoted service path to obtain privilege escalation and stop antimalware services.	https://kcm.trellix.com/corporate/index?page=content&id=SB10404	A-TRE-MOVE-240723/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3438		
Vendor: ui					
Product: unifi					
Affected Version(s): * Up to (excluding) 7.4.156					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Jul-2023	9.1	A backup file vulnerability found in UniFi applications (Version 7.3.83 and earlier) running on Linux operating systems allows application administrators to execute malicious commands on the host device being restored. **CVE ID : CVE-2023-28365**	https://community.ui.com/releases/Security-Advisory-Bulletin-031-031/8c85fc64-e9a8-4082-9ec4-56b14effd545	A-UI-UNIF-240723/517
Product: unifi_network_application					
Affected Version(s): * Up to (including) 7.3.83					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-2023	4.8	A Cross-Site Scripting (XSS) vulnerability found in UniFi Network (Version 7.3.83 and earlier) allows a malicious actor with Site Administrator credentials to escalate privileges by persuading an Administrator to visit a malicious web page. **CVE ID : CVE-2023-32000**	https://community.ui.com/releases/Security-Advisory-Bulletin-034-034/53cfcb84-b42b-4f8f-afbf-07c0ca7cabe2	A-UI-UNIF-240723/518
Vendor: ultimatemember					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ultimate_member					
Affected Version(s): * Up to (excluding) 2.6.7					
Improper Privilege Management	04-Jul-2023	9.8	The Ultimate Member WordPress plugin before 2.6.7 does not prevent visitors from creating user accounts with arbitrary capabilities, effectively allowing attackers to create administrator accounts at will. This is actively being exploited in the wild. **CVE ID : CVE-2023-3460**	https://wpscan.com/vulnerability/694235c7-4469-4ffd-a722-9225b19e98d7	A-ULT-ULTI-240723/519
Vendor: uptime-kuma_project					
Product: uptime-kuma					
Affected Version(s): * Up to (excluding) 1.22.1					
N/A	05-Jul-2023	8.8	Uptime Kuma, a self-hosted monitoring tool, allows an authenticated attacker to install a maliciously crafted plugin in versions prior to 1.22.1, which may lead to remote code execution. Uptime Kuma allows authenticated users to install plugins from an official list of plugins. This feature is currently disabled in the web interface, but the corresponding API	https://github.com/louislam/uptime-kuma/security/advisories/GHSA-7grx-f945-mj96, https://github.com/louislam/uptime-kuma/pull/3346	A-UPT-UPTI-240723/520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints are still available after login. After downloading a plugin, it's installed by calling `npm install` in the installation directory of the plugin. Because the plugin is not validated against the official list of plugins or installed with `npm install --ignore-scripts`, a maliciously crafted plugin taking advantage of npm scripts can gain remote code execution. Version 1.22.1 contains a patch for this issue. **CVE ID : CVE-2023-36821**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jul-2023	8.1	Uptime Kuma, a self-hosted monitoring tool, has a path traversal vulnerability in versions prior to 1.22.1. Uptime Kuma allows authenticated users to install plugins from an official list of plugins. This feature is currently disabled in the web interface, but the corresponding API endpoints are still available after login. Before a plugin is	https://github.com/louislam/uptime-kuma/pull/3346, https://github.com/louislam/uptime-kuma/security/advisories/GHSA-vr8x-74pm-6vj7	A-UPT-UPTI-240723/521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			downloaded, the plugin installation directory is checked for existence. If it exists, it's removed before the plugin installation. Because the plugin is not validated against the official list of plugins or sanitized, the check for existence and the removal of the plugin installation directory are prone to path traversal. This vulnerability allows an authenticated attacker to delete files from the server Uptime Kuma is running on. Depending on which files are deleted, Uptime Kuma or the whole system may become unavailable due to data loss. **CVE ID : CVE-2023-36822**		
Vendor: user_registration_\&_login_and_user_management_system_with_admin_panel_project					
Product: user_registration_\&_login_and_user_management_system_with_admin_panel					
Affected Version(s): 3.0					
Improper Neutralization of Input During Web Page	06-Jul-2023	5.4	A cross-site scripting (XSS) vulnerability in User Registration & Login and User Management System with Admin Panel v3	N/A	A-USE-USER-240723/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the first and last name field. **CVE ID : CVE-2023-27225**		
Vendor: vsourz					
Product: all_in_one_redirection					
Affected Version(s): * Up to (excluding) 2.2.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Jul-2023	7.2	The All In One Redirection WordPress plugin before 2.2.0 does not properly sanitise and escape multiple parameters before using them in an SQL statement, leading to a SQL injection exploitable by high privilege users such as admin. **CVE ID : CVE-2023-2493**	N/A	A-VSO-ALL_-240723/523
Vendor: weather_station_project					
Product: weather_station					
Affected Version(s): * Up to (including) 3.8.12					
Cross-Site Request Forgery (CSRF)	10-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Jason Rouet Weather Station plugin <= 3.8.12 versions. **CVE ID : CVE-2023-25478**	N/A	A-WEA-WEAT-240723/524
Vendor: wedevs					
Product: happy_addons_for_elementor					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 3.8.3					
Cross-Site Request Forgery (CSRF)	10-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in weDevs Happy Addons for Elementor plugin <= 3.8.2 versions. **CVE ID : CVE-2023-28989**	N/A	A-WED-HAPP-240723/525
Vendor: wintercms					
Product: winter					
Affected Version(s): * Up to (excluding) 1.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	4.8	Winter is a free, open-source content management system (CMS) based on the Laravel PHP framework. Users with the `backend.manage_branding` permission can upload SVGs as the application logo. Prior to version 1.2.3, SVG uploads were not sanitized, which could have allowed a stored cross-site scripting (XSS) attack. To exploit the vulnerability, an attacker would already need to have developer or super user level permissions in Winter CMS. This means they would already have extensive access and	https://github.com/wintercms/storm/commit/186d85d8fea2cae43afc807d39f68553c24e56be, https://github.com/wintercms/winter/commit/fa50b4c7489b67ea80072f8ac9fe5294fce1df1c, https://github.com/wintercms/winter/security/advisories/GHSA-wjw2-4j7j-6gc3	A-WIN-WINT-240723/526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control within the system. Additionally, to execute the XSS, the attacker would need to convince the victim to directly visit the URL of the maliciously uploaded SVG, and the application would have to be using local storage where uploaded files are served under the same domain as the application itself instead of a CDN. This is because all SVGs in Winter CMS are rendered through an `img` tag, which prevents any payloads from being executed directly. These two factors significantly limit the potential harm of this vulnerability. This issue has been patched in v1.2.3 through the inclusion of full support for SVG uploads and automatic sanitization of uploaded SVG files. As a workaround, one may apply the patches manually. **CVE ID : CVE-2023-37269**		
Vendor: wpaffiliatemanager					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: affiliates_manager					
Affected Version(s): * Up to (excluding) 2.9.21					
Cross-Site Request Forgery (CSRF)	10-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in wp.Insider, wpaffiliatemgr Affiliates Manager plugin <= 2.9.20 versions. **CVE ID : CVE-2023-28986**	N/A	A-WPA-AFFI-240723/527
Vendor: wpengine					
Product: php_compatibility_checker					
Affected Version(s): * Up to (excluding) 1.6.0					
Cross-Site Request Forgery (CSRF)	11-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WP Engine PHP Compatibility Checker plugin <= 1.5.2 versions. **CVE ID : CVE-2023-24421**	N/A	A-WPE-PHP_-240723/528
Vendor: wpgogo					
Product: custom_field_template					
Affected Version(s): * Up to (excluding) 2.5.9					
Cross-Site Request Forgery (CSRF)	10-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Hiroaki Miyashita Custom Field Template plugin <= 2.5.8 versions. **CVE ID : CVE-2023-22695**	N/A	A-WPG-CUST-240723/529
Vendor: wpplugin					
Product: contact_form_7_redirect_\&_thank_you_page					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.0.4					
Cross-Site Request Forgery (CSRF)	10-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Scott Paterson Contact Form 7 Redirect & Thank You Page plugin <= 1.0.3 versions. **CVE ID : CVE-2023-24395**	N/A	A-WPP-CONT-240723/530
Product: paypal_\&_stripe_add-on					
Affected Version(s): * Up to (excluding) 1.9.4					
Cross-Site Request Forgery (CSRF)	10-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Scott Paterson Contact Form 7 – PayPal & Stripe Add-on plugin <= 1.9.3 versions. **CVE ID : CVE-2023-24405**	N/A	A-WPP-PAYP-240723/531
Vendor: wpzone					
Product: potent_donations_for_woocommerce					
Affected Version(s): * Up to (including) 1.1.9					
Cross-Site Request Forgery (CSRF)	10-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WP Zone Potent Donations for WooCommerce plugin <= 1.1.9 versions. **CVE ID : CVE-2023-35912**	N/A	A-WPZ-POTE-240723/532
Vendor: yontemizleme					
Product: vehicle_tracking_system					
Affected Version(s): * Up to (excluding) 8.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Jul-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Yontem Informatics Vehicle Tracking System allows SQL Injection.This issue affects Vehicle Tracking System: before 8. **CVE ID : CVE-2023-2046**	N/A	A-YON-VEHI-240723/533
Vendor: youtube-dlc_project					
Product: youtube-dlc					
Affected Version(s): *					
URL Redirection to Untrusted Site ('Open Redirect')	06-Jul-2023	8.2	yt-dlp is a command-line program to download videos from video sites. During file downloads, yt-dlp or the external downloaders that yt-dlp employs may leak cookies on HTTP redirects to a different host, or leak them when the host for download fragments differs from their parent manifest's host. This vulnerable behavior is present in yt-dlp prior to 2023.07.06 and nightly	https://github.com/yt-dlp/yt-dlp/commit/3121512228487c9c690d3d39bfd2579addf96e07, https://github.com/yt-dlp/yt-dlp/commit/f8b4bcc0a791274223723488bfbfc23ea3276641, https://github.com/yt-dlp/yt-dlp/security/advisories/	A-YOU-YOUT-240723/534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.07.06.185519. All native and external downloaders are affected, except for `curl` and `httpie` (version 3.1.0 or later). At the file download stage, all cookies are passed by yt-dlp to the file downloader as a `Cookie` header, thereby losing their scope. This also occurs in yt-dlp's info JSON output, which may be used by external tools. As a result, the downloader or external tool may indiscriminately send cookies with requests to domains or paths for which the cookies are not scoped. yt-dlp version 2023.07.06 and nightly 2023.07.06.185519 fix this issue by removing the `Cookie` header upon HTTP redirects; having native downloaders calculate the `Cookie` header from the cookiejar, utilizing	GHSA-v8mc-9377-rwjj	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			external downloaders' built-in support for cookies instead of passing them as header arguments, disabling HTTP redirectiong if the external downloader does not have proper cookie support, processing cookies passed as HTTP headers to limit their scope, and having a separate field for cookies in the info dict storing more information about scoping Some workarounds are available for those who are unable to upgrade. Avoid using cookies and user authentication methods. While extractors may set custom cookies, these usually do not contain sensitive information. Alternatively, avoid using `--load-info-json`. Or, if authentication is a must: verify the integrity of download links from unknown sources in browser (including		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			redirects) before passing them to yt-dlp; use `curl` as external downloader, since it is not impacted; and/or avoid fragmented formats such as HLS/m3u8, DASH/mpd and ISM. **CVE ID : CVE-2023-35934**		
Vendor: yt-dlp_project					
Product: yt-dlp					
Affected Version(s): * Up to (excluding) 2023.07.06					
URL Redirection to Untrusted Site ('Open Redirect')	06-Jul-2023	8.2	yt-dlp is a command-line program to download videos from video sites. During file downloads, yt-dlp or the external downloaders that yt-dlp employs may leak cookies on HTTP redirects to a different host, or leak them when the host for download fragments differs from their parent manifest's host. This vulnerable behavior is present in yt-dlp prior to 2023.07.06 and nightly 2023.07.06.185519. All native and external downloaders are affected, except for `curl` and `httpie`	https://github.com/yt-dlp/yt-dlp/commit/3121512228487c9c690d3d39bfd2579addf96e07, https://github.com/yt-dlp/yt-dlp/commit/f8b4bcc0a791274223723488bfbfc23ea3276641, https://github.com/yt-dlp/yt-dlp/security/advisories/GHSA-v8mc-9377-rwjj	A-YT--YT-D-240723/535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(version 3.1.0 or later). At the file download stage, all cookies are passed by yt-dlp to the file downloader as a `Cookie` header, thereby losing their scope. This also occurs in yt-dlp's info JSON output, which may be used by external tools. As a result, the downloader or external tool may indiscriminately send cookies with requests to domains or paths for which the cookies are not scoped. yt-dlp version 2023.07.06 and nightly 2023.07.06.185519 fix this issue by removing the `Cookie` header upon HTTP redirects; having native downloaders calculate the `Cookie` header from the cookiejar, utilizing external downloaders' built-in support for cookies instead of passing them as header arguments,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disabling HTTP redirectiong if the external downloader does not have proper cookie support, processing cookies passed as HTTP headers to limit their scope, and having a separate field for cookies in the info dict storing more information about scoping Some workarounds are available for those who are unable to upgrade. Avoid using cookies and user authentication methods. While extractors may set custom cookies, these usually do not contain sensitive information. Alternatively, avoid using `--load-info-json`. Or, if authentication is a must: verify the integrity of download links from unknown sources in browser (including redirects) before passing them to yt-dlp; use `curl` as external downloader, since it is not impacted; and/or		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			avoid fragmented formats such as HLS/m3u8, DASH/mpd and ISM. **CVE ID : CVE-2023-35934**		
Affected Version(s): * Up to (excluding) 2023.07.06.185519					
URL Redirection to Untrusted Site ('Open Redirect')	06-Jul-2023	8.2	yt-dlp is a command-line program to download videos from video sites. During file downloads, yt-dlp or the external downloaders that yt-dlp employs may leak cookies on HTTP redirects to a different host, or leak them when the host for download fragments differs from their parent manifest's host. This vulnerable behavior is present in yt-dlp prior to 2023.07.06 and nightly 2023.07.06.185519. All native and external downloaders are affected, except for `curl` and `httpie` (version 3.1.0 or later). At the file download stage, all cookies are passed by yt-dlp to the file downloader as a `Cookie` header,	https://github.com/yt-dlp/yt-dlp/commit/3121512228487c9c690d3d39bfd2579addf96e07, https://github.com/yt-dlp/yt-dlp/commit/f8b4bcc0a791274223723488bfbfc23ea3276641, https://github.com/yt-dlp/yt-dlp/security/advisories/GHSA-v8mc-9377-rwjj	A-YT--YT-D-240723/536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			thereby losing their scope. This also occurs in yt-dlp's info JSON output, which may be used by external tools. As a result, the downloader or external tool may indiscriminately send cookies with requests to domains or paths for which the cookies are not scoped. yt-dlp version 2023.07.06 and nightly 2023.07.06.185519 fix this issue by removing the `Cookie` header upon HTTP redirects; having native downloaders calculate the `Cookie` header from the cookiejar, utilizing external downloaders' built-in support for cookies instead of passing them as header arguments, disabling HTTP redirectiong if the external downloader does not have proper cookie support, processing cookies passed as HTTP headers to limit their		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scope, and having a separate field for cookies in the info dict storing more information about scoping Some workarounds are available for those who are unable to upgrade. Avoid using cookies and user authentication methods. While extractors may set custom cookies, these usually do not contain sensitive information. Alternatively, avoid using `--load-info-json`. Or, if authentication is a must: verify the integrity of download links from unknown sources in browser (including redirects) before passing them to yt-dlp; use `curl` as external downloader, since it is not impacted; and/or avoid fragmented formats such as HLS/m3u8, DASH/mpd and ISM. **CVE ID : CVE-2023-35934**		
Vendor: yzncms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: yzncms					
Affected Version(s): 1.1.0					
Cross-Site Request Forgery (CSRF)	06-Jul-2023	6.5	A Cross-Site Request Forgery (CSRF) in the component /public/admin/profile/update.html of YznCMS v1.1.0 allows attackers to arbitrarily change the Administrator password via a crafted POST request. **CVE ID : CVE-2023-37131**	N/A	A-YZN-YZNC-240723/537
Vendor: Zimbra					
Product: collaboration					
Affected Version(s): 8.8.15					
N/A	06-Jul-2023	9.8	An issue in Zimbra Collaboration (ZCS) v.8.8.15 and v.9.0 allows a remote attacker to escalate privileges and obtain sensitive information via the password and 2FA parameters. **CVE ID : CVE-2023-29381**	https://wiki.zimbra.com/wiki/Security_Center	A-ZIM-COLL-240723/538
N/A	06-Jul-2023	9.8	An issue in Zimbra Collaboration ZCS v.8.8.15 and v.9.0 allows an attacker to execute arbitrary code via the sfdc_preauth.jsp component. **CVE ID : CVE-2023-29382**	https://wiki.zimbra.com/wiki/Security_Center	A-ZIM-COLL-240723/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-2023	9	Cross Site Scripting vulnerability in Zimbra ZCS v.8.8.15 allows a remote authenticated attacker to execute arbitrary code via a crafted script to the /h/autoSaveDraft function. **CVE ID : CVE-2023-34192**	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories, https://wiki.zimbra.com/wiki/Security_Center	A-ZIM-COLL-240723/540
Unrestricted Upload of File with Dangerous Type	06-Jul-2023	8.8	File Upload vulnerability in Zimbra ZCS 8.8.15 allows an authenticated privileged user to execute arbitrary code and obtain sensitive information via the ClientUploader function. **CVE ID : CVE-2023-34193**	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories, https://wiki.zimbra.com/wiki/Security_Center	A-ZIM-COLL-240723/541
Affected Version(s): 9.0.0					
N/A	06-Jul-2023	9.8	An issue in Zimbra Collaboration (ZCS) v.8.8.15 and v.9.0 allows a remote attacker to escalate privileges and obtain sensitive information via the password and 2FA parameters. **CVE ID : CVE-2023-29381**	https://wiki.zimbra.com/wiki/Security_Center	A-ZIM-COLL-240723/542
N/A	06-Jul-2023	9.8	An issue in Zimbra Collaboration ZCS v.8.8.15 and v.9.0 allows an attacker to	https://wiki.zimbra.com/	A-ZIM-COLL-240723/543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code via the sfdc_preauth.jsp component. **CVE ID : CVE-2023-29382**	wiki/Security_Center	
Vendor: Zohocorp					
Product: manageengine_adaudit_plus					
Affected Version(s): * Up to (excluding) 7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	5.4	Zoho ManageEngine ADAudit Plus before 7100 allows XSS via the username field. **CVE ID : CVE-2023-37308**	https://www.manageengine.com/products/active-directory-audit/cve-2023-37308.html	A-ZOH-MANA-240723/544
Affected Version(s): 7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	5.4	Zoho ManageEngine ADAudit Plus before 7100 allows XSS via the username field. **CVE ID : CVE-2023-37308**	https://www.manageengine.com/products/active-directory-audit/cve-2023-37308.html	A-ZOH-MANA-240723/545
Product: manageengine_admanager_plus					
Affected Version(s): * Up to (excluding) 7.1					
Improper Restriction of XML External Entity Reference	05-Jul-2023	4.9	Zoho ManageEngine ADManager Plus before 7183 allows admin users to exploit an XXE issue to view files. **CVE ID : CVE-2023-35786**	https://www.manageengine.com/products/ad-manager/admanager-kb/cve-2023-35786.html	A-ZOH-MANA-240723/546
Affected Version(s): 7.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of XML External Entity Reference	05-Jul-2023	4.9	Zoho ManageEngine ADManager Plus before 7183 allows admin users to exploit an XXE issue to view files. **CVE ID : CVE-2023-35786**	https://www.manageengine.com/products/ad-manager/admanager-kb/cve-2023-35786.html	A-ZOH-MANA-240723/547
Product: manageengine_servicedesk_plus					
Affected Version(s): * Up to (excluding) 14.2					
N/A	07-Jul-2023	5.4	Zoho ManageEngine ServiceDesk Plus before 14202, ServiceDesk Plus MSP before 14300, and SupportCenter Plus before 14300 have a privilege escalation vulnerability in the Release module that allows unprivileged users to access the Reminders of a release ticket and make modifications. **CVE ID : CVE-2023-34197**	https://www.manageengine.com/products/service-desk/CVE-2023-34197.html	A-ZOH-MANA-240723/548
Affected Version(s): 14.2					
N/A	07-Jul-2023	5.4	Zoho ManageEngine ServiceDesk Plus before 14202, ServiceDesk Plus MSP before 14300, and SupportCenter Plus before 14300 have a privilege escalation vulnerability in the Release module that allows unprivileged	https://www.manageengine.com/products/service-desk/CVE-2023-34197.html	A-ZOH-MANA-240723/549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			users to access the Reminders of a release ticket and make modifications. **CVE ID : CVE-2023-34197**		
Product: manageengine_servicedesk_plus_msp					
Affected Version(s): * Up to (excluding) 14.2					
N/A	07-Jul-2023	5.4	Zoho ManageEngine ServiceDesk Plus before 14202, ServiceDesk Plus MSP before 14300, and SupportCenter Plus before 14300 have a privilege escalation vulnerability in the Release module that allows unprivileged users to access the Reminders of a release ticket and make modifications. **CVE ID : CVE-2023-34197**	https://www.manageengine.com/products/service-desk/CVE-2023-34197.html	A-ZOH-MANA-240723/550
Affected Version(s): 14.2					
N/A	07-Jul-2023	5.4	Zoho ManageEngine ServiceDesk Plus before 14202, ServiceDesk Plus MSP before 14300, and SupportCenter Plus before 14300 have a privilege escalation vulnerability in the Release module that allows unprivileged users to access the Reminders of a	https://www.manageengine.com/products/service-desk/CVE-2023-34197.html	A-ZOH-MANA-240723/551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			release ticket and make modifications. **CVE ID : CVE-2023-34197**		
Product: manageengine_supportcenter_plus					
Affected Version(s): * Up to (excluding) 14.2					
N/A	07-Jul-2023	5.4	Zoho ManageEngine ServiceDesk Plus before 14202, ServiceDesk Plus MSP before 14300, and SupportCenter Plus before 14300 have a privilege escalation vulnerability in the Release module that allows unprivileged users to access the Reminders of a release ticket and make modifications. **CVE ID : CVE-2023-34197**	https://www.manageengine.com/products/service-desk/CVE-2023-34197.html	A-ZOH-MANA-240723/552
Affected Version(s): 14.2					
N/A	07-Jul-2023	5.4	Zoho ManageEngine ServiceDesk Plus before 14202, ServiceDesk Plus MSP before 14300, and SupportCenter Plus before 14300 have a privilege escalation vulnerability in the Release module that allows unprivileged users to access the Reminders of a release ticket and make modifications.	https://www.manageengine.com/products/service-desk/CVE-2023-34197.html	A-ZOH-MANA-240723/553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34197		
Vendor: zzcms					
Product: zzcms					
Affected Version(s): 2023					
Cross-Site Request Forgery (CSRF)	03-Jul-2023	8.8	Cross Site Request Forgery vulnerability in ZZCMS v.2023 alows a remote attacker to gain privileges via the add function in adminlist.php. **CVE ID : CVE-2023-36162**	N/A	A-ZZC-ZZCM-240723/554
Hardware					
Vendor: Arubanetworks					
Product: mcr-hw-10k					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jul-2023	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-35975**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/555
Buffer Copy without Checking Size of Input ('Classic	05-Jul-2023	7.5	There is an unauthenticated buffer overflow vulnerability in the process controlling the ArubaOS web-based	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			management interface. Successful exploitation of this vulnerability results in a Denial-of-Service (DoS) condition affecting the web-based management interface of the controller. **CVE ID : CVE-2023-35979**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	An authenticated remote command injection vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-35972**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/557
Improper Neutralization of Special Elements used in a Command ('Comman	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35973**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35974**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/559
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35976		
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35977**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/561
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in the ArubaOS web-based management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35971**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/562
Improper Neutralization of	05-Jul-2023	6.1	A vulnerability in ArubaOS could allow an	https://www.arubanetworks.com/as	H-ARU-MCR--240723/563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			unauthenticated remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based management interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35978**	sets/alert/ARUBA-PSA-2023-008.txt	
Product: mcr-hw-1k					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jul-2023	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-35975**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/564
Buffer Copy without Checking Size of Input ('Classic	05-Jul-2023	7.5	There is an unauthenticated buffer overflow vulnerability in the process controlling the ArubaOS web-based management interfac	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			e. Successful exploitation of this vulnerability results in a Denial-of-Service (DoS) condition affecting the web-based management interface of the controller. **CVE ID : CVE-2023-35979**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	An authenticated remote command injection vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-35972**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/566
Improper Neutralization of Special Elements used in a Command ('Comman	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35973**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35974**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/568
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35976**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35977**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/570
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in the ArubaOS web-based management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35971**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/571
Improper Neutralization of Input During Web Page	05-Jul-2023	6.1	A vulnerability in ArubaOS could allow an unauthenticated remote attacker to conduct a reflected	https://www.arubanetworks.com/assets/alert/A	H-ARU-MCR--240723/572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			cross-site scripting (XSS) attack against a user of the web-based management interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35978**	RUBA-PSA-2023-008.txt	
Product: mcr-hw-5k					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jul-2023	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-35975**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/573
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jul-2023	7.5	There is an unauthenticated buffer overflow vulnerability in the process controlling the ArubaOS web-based management interface. Successful exploitation of this vulnerability results	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in a Denial-of-Service (DoS) condition affecting the web-based management interface of the controller. **CVE ID : CVE-2023-35979**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	An authenticated remote command injection vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-35972**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/575
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system. **CVE ID : CVE-2023-35973**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35974**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/577
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35976**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/578
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated	https://www.arubanetworks.com/as	H-ARU-MCR--240723/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35977**	sets/alert/ARUBA-PSA-2023-008.txt	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in the ArubaOS web-based management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35971**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/580
Improper Neutralization of Input During Web Page Generation	05-Jul-2023	6.1	A vulnerability in ArubaOS could allow an unauthenticated remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	H-ARU-MCR--240723/581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			of the web-based management interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35978**		
Vendor: Cisco					
Product: nexus_9000_in_aci_mode					
Affected Version(s): -					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	H-CIS-NEXU-240723/582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Vendor: heroelectronix					
Product: qubo_hcd01					
Affected Version(s): -					
Missing Authentication for Critical Function	04-Jul-2023	8.8	Hero Qubo HCD01_02_V1.38_20220125 devices allow TELNET access with root privileges by default, without a password. **CVE ID : CVE-2023-22906**	N/A	H-HER-QUBO-240723/583
Product: qubo_hcd02					
Affected Version(s): -					
Missing Authentication for Critical Function	04-Jul-2023	8.8	Hero Qubo HCD01_02_V1.38_20220125 devices allow TELNET access with root privileges by default, without a password.	N/A	H-HER-QUBO-240723/584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22906		
Vendor: loxone					
Product: miniserver_go_gen_2					
Affected Version(s): -					
Use of Hard-coded Credentials	05-Jul-2023	7.8	The root password of the Loxone Miniserver Go Gen.2 before 14.2 is calculated using hard-coded secrets and the MAC address. This allows a local user to calculate the root password and escalate privileges. **CVE ID : CVE-2023-36623**	N/A	H-LOX-MINI-240723/585
Missing Authorization	05-Jul-2023	7.8	Loxone Miniserver Go Gen.2 through 14.0.3.28 allows an authenticated operating system user to escalate privileges via the Sudo configuration. This allows the elevated execution of binaries without a password requirement. **CVE ID : CVE-2023-36624**	N/A	H-LOX-MINI-240723/586
Improper Neutralization of Special Elements used in an OS	05-Jul-2023	7.2	The websocket configuration endpoint of the Loxone Miniserver Go Gen.2 before 14.1.5.9 allows remote	N/A	H-LOX-MINI-240723/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			authenticated administrators to inject arbitrary OS commands via the timezone parameter. **CVE ID : CVE-2023-36622**		
Vendor: mediatek					
Product: mt6580					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT65-240723/588
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT65-240723/589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**		
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT65-240723/590
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT65-240723/591
Integer Overflow or	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow.	https://corp.mediatek.com/product-security-	H-MED-MT65-240723/592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT65-240723/593
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT65-240723/594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**		
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT65-240723/595
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Jul-2023	6.4	In display, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671046; Issue ID: ALPS07671046. **CVE ID : CVE-2023-20771**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT65-240723/596
Product: mt6731					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/597
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/598
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/600
Product: mt6735					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**		
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/602
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/603
Integer Overflow or	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT67-240723/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	security-bulletin/July-2023	
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/605
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**		
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/607
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/608
Product: mt6737					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/609
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/610
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/612
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**		
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/614
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/615
Product: mt6739					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/616
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664741; Issue ID: ALPS07664741. **CVE ID : CVE-2023-20689**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/617
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664735; Issue ID: ALPS07664735. **CVE ID : CVE-2023-20690**		
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664731; Issue ID: ALPS07664731. **CVE ID : CVE-2023-20691**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/619
Improper Handling of Exceptional Conditions	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664720; Issue ID: ALPS07664720.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20692		
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664711; Issue ID: ALPS07664711. **CVE ID : CVE-2023-20693**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/621
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/622
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/624
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**		
Out-of-bounds Write	04-Jul-2023	6.7	In cmdq, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636133. **CVE ID : CVE-2023-20757**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/626
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/628
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/629
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**		
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/631
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Jul-2023	6.4	In display, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671046;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07671046. **CVE ID : CVE-2023-20771**		
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130. **CVE ID : CVE-2023-20758**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/633
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601. **CVE ID : CVE-2023-20759**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/634
Product: mt6753					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/635
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/636
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/638
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20756		
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/640
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/641
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-240723/642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	bulletin/July-2023	
Product: mt6757					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/643
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/645
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/647
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/648
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**		
Product: mt6757c					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/650
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/652
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/653
Access of Resource Using Incompatib	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This	https://corp.mediatek.com/product-security-	H-MED-MT67-240723/654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
le Type ('Type Confusion')			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/655
Product: mt6757cd					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**		
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/657
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/659
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/660
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**		
Product: mt6757ch					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/662
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/664
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/665
Access of Resource Using Incompatib	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This	https://corp.mediatek.com/product-security-	H-MED-MT67-240723/666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
le Type ('Type Confusion')			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/667
Product: mt6761					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**		
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/669
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20754		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/671
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/672
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**		
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/674
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**		
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/676
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/677
Concurrent Execution	04-Jul-2023	6.4	In display, there is a possible memory	https://corp.mediatek.co	H-MED-MT67-240723/678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671046; Issue ID: ALPS07671046. **CVE ID : CVE-2023-20771**	m/product-security-bulletin/July-2023	
Product: mt6762					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/679
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/681
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20756		
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/683
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/684
Access of Resource Using Incompatib	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This	https://corp.mediatek.com/product-security-	H-MED-MT67-240723/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
le Type ('Type Confusion')			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	bulletin/July-2023	
Product: mt6763					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/686
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/688
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/690
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/691
Access of Resource Using Incompatible Type	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**		
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/693
Product: mt6765					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**		
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/695
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/696
Integer Overflow	04-Jul-2023	6.7	In keyinstall, there is a possible out of	https://corp.mediatek.co	H-MED-MT67-240723/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	m/product-security-bulletin/July-2023	
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/698
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**		
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/700
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/702
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/703
Concurrent Execution using Shared Resource with Improper	04-Jul-2023	6.4	In display, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671046; Issue ID: ALPS07671046. **CVE ID : CVE-2023-20771**		
Product: mt6768					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/705
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**		
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/707
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/708
Integer Overflow or	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT67-240723/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	security-bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In cmdq, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636133. **CVE ID : CVE-2023-20757**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/710
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**		
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/712
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/714
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/715
Concurrent Execution using Shared Resource with Improper	04-Jul-2023	6.4	In display, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671046; Issue ID: ALPS07671046. **CVE ID : CVE-2023-20771**		
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130. **CVE ID : CVE-2023-20758**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/717
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20759		
Product: mt6769					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/719
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/720
Integer Overflow or	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow.	https://corp.mediatek.com/product-security-	H-MED-MT67-240723/721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	bulletin/July-2023	
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/722
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**		
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/724
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/725
Product: mt6771					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/726
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/727
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/729
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**		
Out-of-bounds Write	04-Jul-2023	6.7	In cmdq, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636133. **CVE ID : CVE-2023-20757**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/731
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/733
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/734
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**		
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/736
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Jul-2023	6.4	In display, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671046;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07671046. **CVE ID : CVE-2023-20771**		
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130. **CVE ID : CVE-2023-20758**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/738
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601. **CVE ID : CVE-2023-20759**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/739
Product: mt6779					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/740
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/741
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/743
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20756		
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/745
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/746
Access of Resource Using Incompatib	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This	https://corp.mediatek.com/product-security-	H-MED-MT67-240723/747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
le Type ('Type Confusion')			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	bulletin/July-2023	
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/748
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Jul-2023	6.4	In display, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671046; Issue ID: ALPS07671046. **CVE ID : CVE-2023-20771**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/750
Product: mt6781					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20773		
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/752
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/753
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/755
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**		
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/757
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/758
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a	https://corp.mediatek.com/product-	H-MED-MT67-240723/759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	security-bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/760
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130. **CVE ID : CVE-2023-20758**		
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601. **CVE ID : CVE-2023-20759**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/762
Product: mt6785					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20773		
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/764
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/765
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/767
Out-of-bounds Write	04-Jul-2023	6.7	In cmdq, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07636133. **CVE ID : CVE-2023-20757**		
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/769
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/770
Access of Resource	04-Jul-2023	6.7	In ion, there is a possible out of	https://corp.mediatek.co	H-MED-MT67-240723/771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Using Incompatible Type ('Type Confusion')			bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	m/product-security-bulletin/July-2023	
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/772
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Jul-2023	6.4	In display, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671046; Issue ID: ALPS07671046. **CVE ID : CVE-2023-20771**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/774
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130. **CVE ID : CVE-2023-20758**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601. **CVE ID : CVE-2023-20759**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/776
Product: mt6789					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/777
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT67-240723/778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/779
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/781
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/782
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT67-240723/783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	security-bulletin/July-2023	
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/784
Out-of-bounds Read	04-Jul-2023	6.7	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07292228; Issue ID: ALPS07292228. **CVE ID : CVE-2023-20774**		
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT67-240723/786
Product: mt6833					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**		
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/788
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/789
Integer Overflow or	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow.	https://corp.mediatek.com/product-security-	H-MED-MT68-240723/790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	bulletin/July-2023	
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/791
Out-of-bounds Write	04-Jul-2023	6.7	In cmdq, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07636133; Issue ID: ALPS07636133. **CVE ID : CVE-2023-20757**		
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/793
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/795
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/796
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**		
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130. **CVE ID : CVE-2023-20758**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/798
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20759		
Product: mt6835					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/800
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/802
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/803
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**		
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/805
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20772		
Out-of-bounds Read	04-Jul-2023	6.7	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07292228; Issue ID: ALPS07292228. **CVE ID : CVE-2023-20774**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/807
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/808
Product: mt6853					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/809
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/810
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/812
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20756		
Out-of-bounds Write	04-Jul-2023	6.7	In cmdq, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636133. **CVE ID : CVE-2023-20757**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/814
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/815
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-240723/816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	bulletin/July-2023	
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/817
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**		
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/819
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130. **CVE ID : CVE-2023-20758**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601. **CVE ID : CVE-2023-20759**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/821
Product: mt6853t					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/822
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT68-240723/823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/824
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/826
Out-of-bounds Write	04-Jul-2023	6.7	In cmdq, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636133. **CVE ID : CVE-2023-20757**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/827
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT68-240723/828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	security-bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/829
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**		
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/831
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20775		
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130. **CVE ID : CVE-2023-20758**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/833
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601. **CVE ID : CVE-2023-20759**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/834
Product: mt6855					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission	https://corp.mediatek.com/product-security-	H-MED-MT68-240723/835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/836
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/838
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/839
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT68-240723/840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	security-bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/841
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**		
Out-of-bounds Read	04-Jul-2023	6.7	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07292228; Issue ID: ALPS07292228. **CVE ID : CVE-2023-20774**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/843
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20775		
Product: mt6873					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/845
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/847
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/848
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**		
Out-of-bounds Write	04-Jul-2023	6.7	In cmdq, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636133. **CVE ID : CVE-2023-20757**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/850
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20761		
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/852
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/853
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-240723/854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/855
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07636133; Issue ID: ALPS07636130. **CVE ID : CVE-2023-20758**		
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601. **CVE ID : CVE-2023-20759**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/857
Product: mt6875					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/859
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/860
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**		
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/862
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20766		
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/864
Product: mt6877					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/866
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/867
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/869
Out-of-bounds Write	04-Jul-2023	6.7	In cmdq, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636133.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20757		
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/871
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/872
Access of Resource Using Incompatib	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This	https://corp.mediatek.com/product-security-	H-MED-MT68-240723/873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
le Type ('Type Confusion')			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	bulletin/July-2023	
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/874
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**		
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130. **CVE ID : CVE-2023-20758**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/876
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601. **CVE ID : CVE-2023-20759**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/877
Product: mt6879					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/878
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/879
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/881
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**		
Out-of-bounds Write	04-Jul-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629578; Issue ID: ALPS07629578. **CVE ID : CVE-2023-20760**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/883
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/885
Out-of-bounds Write	04-Jul-2023	6.7	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585; Issue ID: ALPS07629584. **CVE ID : CVE-2023-20767**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/886
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**		
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/888
Out-of-bounds Read	04-Jul-2023	4.4	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07536951;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07536951. **CVE ID : CVE-2023-20748**		
Product: mt6883					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/890
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/892
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/893
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**		
Out-of-bounds Write	04-Jul-2023	6.7	In cmdq, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636133. **CVE ID : CVE-2023-20757**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/895
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20761		
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/897
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/898
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-240723/899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130. **CVE ID : CVE-2023-20758**	bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601. **CVE ID : CVE-2023-20759**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/900
Product: mt6885					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**		
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/902
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/904
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/905
Out-of-bounds Write	04-Jul-2023	6.7	In cmdq, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636133. **CVE ID : CVE-2023-20757**		
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/907
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20768		
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/909
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/910
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-240723/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130. **CVE ID : CVE-2023-20758**	bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601. **CVE ID : CVE-2023-20759**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/912
Product: mt6886					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**		
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/914
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/916
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/917
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**		
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/919
Out-of-bounds Write	04-Jul-2023	6.7	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07629584. **CVE ID : CVE-2023-20767**		
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/921
Out-of-bounds Read	04-Jul-2023	6.7	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07292228; Issue ID: ALPS07292228. **CVE ID : CVE-2023-20774**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/923
Out-of-bounds Read	04-Jul-2023	4.4	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07536951; Issue ID: ALPS07536951. **CVE ID : CVE-2023-20748**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/924
Product: mt6889					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission	https://corp.mediatek.com/product-security-	H-MED-MT68-240723/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/926
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/928
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/929
Out-of-bounds Write	04-Jul-2023	6.7	In cmdq, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT68-240723/930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636133. **CVE ID : CVE-2023-20757**	security-bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/931
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**		
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/933
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20775		
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130. **CVE ID : CVE-2023-20758**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/935
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601. **CVE ID : CVE-2023-20759**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/936
Product: mt6890					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-240723/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	bulletin/July-2023	
Product: mt6891					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/938
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/940
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/942
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/943
Access of Resource Using Incompatible Type	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**		
Product: mt6893					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/945
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**		
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/947
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/948
Integer Overflow or	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT68-240723/949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	security-bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In cmdq, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636133. **CVE ID : CVE-2023-20757**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/950
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**		
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/952
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/954
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/955
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130. **CVE ID : CVE-2023-20758**		
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601. **CVE ID : CVE-2023-20759**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/957
Product: mt6895					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**		
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664711; Issue ID: ALPS07664711. **CVE ID : CVE-2023-20693**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/959
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/960
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT68-240723/961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	security-bulletin/July-2023	
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/962
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**		
Out-of-bounds Write	04-Jul-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629578; Issue ID: ALPS07629578. **CVE ID : CVE-2023-20760**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/964
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/966
Out-of-bounds Write	04-Jul-2023	6.7	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585; Issue ID: ALPS07629584. **CVE ID : CVE-2023-20767**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/967
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**		
Out-of-bounds Read	04-Jul-2023	6.7	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07292228; Issue ID: ALPS07292228. **CVE ID : CVE-2023-20774**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/969
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**		
Out-of-bounds Read	04-Jul-2023	4.4	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07536951; Issue ID: ALPS07536951. **CVE ID : CVE-2023-20748**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT68-240723/971
Product: mt6983					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20773		
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664711; Issue ID: ALPS07664711. **CVE ID : CVE-2023-20693**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/973
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/974
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/976
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**		
Out-of-bounds Write	04-Jul-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629578; Issue ID: ALPS07629578. **CVE ID : CVE-2023-20760**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/978
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/980
Out-of-bounds Write	04-Jul-2023	6.7	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585; Issue ID: ALPS07629584. **CVE ID : CVE-2023-20767**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/981
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**		
Out-of-bounds Read	04-Jul-2023	6.7	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07292228; Issue ID: ALPS07292228. **CVE ID : CVE-2023-20774**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/983
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**		
Out-of-bounds Read	04-Jul-2023	4.4	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07536951; Issue ID: ALPS07536951. **CVE ID : CVE-2023-20748**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/985
Product: mt6985					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20773		
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/987
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/988
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/990
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**		
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/992
Out-of-bounds Write	04-Jul-2023	6.7	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585; Issue ID: ALPS07629584. **CVE ID : CVE-2023-20767**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/994
Out-of-bounds Read	04-Jul-2023	6.7	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07292228; Issue ID: ALPS07292228. **CVE ID : CVE-2023-20774**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/995
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**		
Out-of-bounds Read	04-Jul-2023	4.4	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07536951; Issue ID: ALPS07536951. **CVE ID : CVE-2023-20748**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/997
Product: mt6990					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT69-240723/998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**		
Product: mt8167					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664741; Issue ID: ALPS07664741. **CVE ID : CVE-2023-20689**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/999
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664735; Issue ID: ALPS07664735.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20690		
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664731; Issue ID: ALPS07664731. **CVE ID : CVE-2023-20691**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1001
Improper Handling of Exceptional Conditions	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664720; Issue ID: ALPS07664720. **CVE ID : CVE-2023-20692**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1002
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664711; Issue ID: ALPS07664711. **CVE ID : CVE-2023-20693**		
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1004
Out-of-bounds Write	04-Jul-2023	6.7	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07629584. **CVE ID : CVE-2023-20767**		
Product: mt8168					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664735; Issue ID: ALPS07664735. **CVE ID : CVE-2023-20690**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1006
Improper Handling of Exceptional Conditions	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664720; Issue ID: ALPS07664720. **CVE ID : CVE-2023-20692**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664711; Issue ID: ALPS07664711. **CVE ID : CVE-2023-20693**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1008
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1009
Out-of-bounds Write	04-Jul-2023	6.7	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585; Issue ID: ALPS07629584. **CVE ID : CVE-2023-20767**		
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1011
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Jul-2023	6.4	In display, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671046; Issue ID: ALPS07671046. **CVE ID : CVE-2023-20771**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1013
Product: mt8173					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt8175					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1015
Product: mt8183					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1016
Product: mt8185					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1017
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1018
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1020
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**		
Product: mt8195					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664711; Issue ID: ALPS07664711. **CVE ID : CVE-2023-20693**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1022
Out-of-bounds Write	04-Jul-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629578; Issue ID: ALPS07629578. **CVE ID : CVE-2023-20760**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585; Issue ID: ALPS07629584. **CVE ID : CVE-2023-20767**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1024
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1025
Out-of-bounds Read	04-Jul-2023	6.7	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07292228; Issue ID: ALPS07292228. **CVE ID : CVE-2023-20774**		
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT81-240723/1027
Product: mt8321					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07664741; Issue ID: ALPS07664741. **CVE ID : CVE-2023-20689**		
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664735; Issue ID: ALPS07664735. **CVE ID : CVE-2023-20690**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1029
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664731; Issue ID: ALPS07664731. **CVE ID : CVE-2023-20691**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1030
Improper Handling of	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to	https://corp.mediatek.com/product-	H-MED-MT83-240723/1031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664720; Issue ID: ALPS07664720. **CVE ID : CVE-2023-20692**	security-bulletin/July-2023	
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664711; Issue ID: ALPS07664711. **CVE ID : CVE-2023-20693**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1032
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**		
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1034
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1035
Integer Overflow or	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT83-240723/1036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	security-bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1037
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**		
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1039
Product: mt8362a					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20766		
Product: mt8365					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664741; Issue ID: ALPS07664741. **CVE ID : CVE-2023-20689**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1041
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664735; Issue ID: ALPS07664735. **CVE ID : CVE-2023-20690**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1042
Integer Overflow or	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow.	https://corp.mediatek.com/product-security-	H-MED-MT83-240723/1043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664731; Issue ID: ALPS07664731. **CVE ID : CVE-2023-20691**	bulletin/July-2023	
Improper Handling of Exceptional Conditions	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664720; Issue ID: ALPS07664720. **CVE ID : CVE-2023-20692**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1044
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664711;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07664711. **CVE ID : CVE-2023-20693**		
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1046
Product: mt8385					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664741; Issue ID: ALPS07664741. **CVE ID : CVE-2023-20689**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664735; Issue ID: ALPS07664735. **CVE ID : CVE-2023-20690**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1048
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664731; Issue ID: ALPS07664731. **CVE ID : CVE-2023-20691**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1049
Improper Handling of Exceptional Conditions	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07664720; Issue ID: ALPS07664720. **CVE ID : CVE-2023-20692**		
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664711; Issue ID: ALPS07664711. **CVE ID : CVE-2023-20693**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1051
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1053
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1054
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**		
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT83-240723/1056
Product: mt8666					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664741;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07664741. **CVE ID : CVE-2023-20689**		
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664735; Issue ID: ALPS07664735. **CVE ID : CVE-2023-20690**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1058
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664731; Issue ID: ALPS07664731. **CVE ID : CVE-2023-20691**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1059
Improper Handling of Exceptiona	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught	https://corp.mediatek.com/product-security-	H-MED-MT86-240723/1060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664720; Issue ID: ALPS07664720. **CVE ID : CVE-2023-20692**	bulletin/July-2023	
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664711; Issue ID: ALPS07664711. **CVE ID : CVE-2023-20693**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1061
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**		
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1063
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1064
Integer Overflow or	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow.	https://corp.mediatek.com/product-security-	H-MED-MT86-240723/1065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1066
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**		
Product: mt8667					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1068
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1070
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1071
Product: mt8673					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT86-240723/1072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585; Issue ID: ALPS07629584. **CVE ID : CVE-2023-20767**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1073
Out-of-bounds Read	04-Jul-2023	6.7	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07292228; Issue ID: ALPS07292228. **CVE ID : CVE-2023-20774**		
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1075
Out-of-bounds Read	04-Jul-2023	4.4	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07536951; Issue ID: ALPS07536951. **CVE ID : CVE-2023-20748**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1076
Product: mt8675					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1077
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1078
Access of Resource Using Incompatible Type	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT86-240723/1079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**		
Product: mt8765					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664741; Issue ID: ALPS07664741. **CVE ID : CVE-2023-20689**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1080
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07664735; Issue ID: ALPS07664735. **CVE ID : CVE-2023-20690**		
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664731; Issue ID: ALPS07664731. **CVE ID : CVE-2023-20691**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1082
Improper Handling of Exceptional Conditions	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664720; Issue ID: ALPS07664720. **CVE ID : CVE-2023-20692**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1083
Integer Overflow or	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to	https://corp.mediatek.com/product-	H-MED-MT87-240723/1084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664711; Issue ID: ALPS07664711. **CVE ID : CVE-2023-20693**	security-bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1085
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1087
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1088
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT87-240723/1089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	security-bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1090
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**		
Product: mt8766					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1092
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20754		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1094
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1095
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**		
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1097
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**		
Product: mt8768					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1099
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1101
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1102
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**		
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1104
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20768		
Product: mt8781					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1106
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664711; Issue ID: ALPS07664711. **CVE ID : CVE-2023-20693**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1108
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1109
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1111
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20761		
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1113
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1114
Out-of-bounds Read	04-Jul-2023	6.7	In display, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT87-240723/1115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07292228; Issue ID: ALPS07292228. **CVE ID : CVE-2023-20774**	bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1116
Concurrent Execution using Shared Resource with Improper Synchronization	04-Jul-2023	6.4	In display, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			exploitation. Patch ID: ALPS07671046; Issue ID: ALPS07671046. **CVE ID : CVE-2023-20771**		
Out-of-bounds Read	04-Jul-2023	4.4	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07536951; Issue ID: ALPS07536951. **CVE ID : CVE-2023-20748**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1118
Product: mt8786					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20753		
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1120
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1121
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**		
Out-of-bounds Write	04-Jul-2023	6.7	In cmdq, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636133. **CVE ID : CVE-2023-20757**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1123
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**		
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1125
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1126
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a	https://corp.mediatek.com/product-	H-MED-MT87-240723/1127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130. **CVE ID : CVE-2023-20758**	security-bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601. **CVE ID : CVE-2023-20759**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1128
Product: mt8788					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07664741; Issue ID: ALPS07664741. **CVE ID : CVE-2023-20689**		
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664735; Issue ID: ALPS07664735. **CVE ID : CVE-2023-20690**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1130
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664731; Issue ID: ALPS07664731. **CVE ID : CVE-2023-20691**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664720; Issue ID: ALPS07664720. **CVE ID : CVE-2023-20692**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1132
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664711; Issue ID: ALPS07664711. **CVE ID : CVE-2023-20693**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1133
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**		
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1135
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1137
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1138
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**		
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1140
Product: mt8789					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**		
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1142
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1143
Integer Overflow or	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow.	https://corp.mediatek.com/product-security-	H-MED-MT87-240723/1144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In cmdq, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636133. **CVE ID : CVE-2023-20757**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1145
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**		
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1147
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130. **CVE ID : CVE-2023-20758**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601. **CVE ID : CVE-2023-20759**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1149
Product: mt8791					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1150
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to	https://corp.mediatek.com/product-security-	H-MED-MT87-240723/1151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	bulletin/July-2023	
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1152
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**		
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1154
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1156
Product: mt8791t					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1157
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This	https://corp.mediatek.com/product-security-	H-MED-MT87-240723/1158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1159
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1161
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1162
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT87-240723/1163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	security-bulletin/July-2023	
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1164
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**		
Product: mt8797					
Affected Version(s): -					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1166
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667.	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20753		
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1168
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1169
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**		
Out-of-bounds Write	04-Jul-2023	6.7	In cmdq, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636133. **CVE ID : CVE-2023-20757**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1171
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604;	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**		
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1173
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1174
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a	https://corp.mediatek.com/product-	H-MED-MT87-240723/1175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	security-bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130. **CVE ID : CVE-2023-20758**	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1176
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2023	H-MED-MT87-240723/1177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601. **CVE ID : CVE-2023-20759**		
Vendor: milesight					
Product: ur-32l					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jul-2023	9.8	A stack-based buffer overflow vulnerability exists in the libzebra.so.0.0.0 security_decrypt_password functionality of Milesight UR32L v32.3.0.5. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2023-24018**	N/A	H-MIL-UR-3-240723/1178
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these	N/A	H-MIL-UR-3-240723/1179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities.This buffer overflow occurs in the set_qos function with the attach_class variable. **CVE ID : CVE-2023-25097**		
Product: ur32l					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jul-2023	9.8	A buffer overflow vulnerability exists in the uhttpd login functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to remote code execution. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2023-23902**	N/A	H-MIL-UR32-240723/1180
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jul-2023	9.8	An OS command injection vulnerability exists in the vtysh_ubus tcpdump_start_cb functionality of Milesight UR32L v32.3.0.5. A specially crafted HTTP request can lead to command execution. An attacker can send an HTTP request to trigger this vulnerability.	N/A	H-MIL-UR32-240723/1181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22653		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jul-2023	8.8	An OS command injection vulnerability exists in the vtysh_ubus _get_fw_logs functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to command execution. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2023-22299**	N/A	H-MIL-UR32-240723/1182
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jul-2023	8.8	Two OS command injection vulnerability exist in the vtysh_ubus toolsh_excute.constprop.1 functionality of Milesight UR32L v32.3.0.5. A specially-crafted network request can lead to command execution. An attacker can send a network request to trigger these vulnerabilities.This command injection is in the ping tool utility. **CVE ID : CVE-2023-24519**	N/A	H-MIL-UR32-240723/1183
Improper Neutralizat	06-Jul-2023	8.8	Two OS command injection	N/A	H-MIL-UR32-240723/1184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			vulnerability exist in the vtysh_ubus toolsh_excute.constprop.1 functionality of Milesight UR32L v32.3.0.5. A specially-crafted network request can lead to command execution. An attacker can send a network request to trigger these vulnerabilities.This command injection is in the trace tool utility. **CVE ID : CVE-2023-24520**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jul-2023	8.8	Two OS command injection vulnerabilities exist in the urvpn_client cmd_name_action functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to arbitrary command execution. An attacker can send a network request to trigger these vulnerabilities.This OS command injection is triggered through a UDP packet. **CVE ID : CVE-2023-24583**	N/A	H-MIL-UR32-240723/1185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jul-2023	8.8	Two OS command injection vulnerabilities exist in the urvpn_client cmd_name_action functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to arbitrary command execution. An attacker can send a network request to trigger these vulnerabilities.This OS command injection is triggered through a TCP packet. **CVE ID : CVE-2023-24582**	N/A	H-MIL-UR32-240723/1186
Out-of-bounds Write	06-Jul-2023	8.1	A stack-based buffer overflow vulnerability exists in the urvpn_client http_connection_readcb functionality of Milesight UR32L v32.3.0.5. A specially crafted network packet can lead to a buffer overflow. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2023-24019**	N/A	H-MIL-UR32-240723/1187
Improper Certificate Validation	06-Jul-2023	8.1	A misconfiguration vulnerability exists in the urvpn_client functionality of	N/A	H-MIL-UR32-240723/1188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Milesight UR32L v32.3.0.5. A specially-crafted man-in-the-middle attack can lead to increased privileges. An attacker can perform a man-in-the-middle attack to trigger this vulnerability. **CVE ID : CVE-2023-23546**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_pptp function with the remote_subnet and the remote_mask variables. **CVE ID : CVE-2023-25119**	N/A	H-MIL-UR32-240723/1189
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight	N/A	H-MIL-UR32-240723/1190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_dmvpn function with the cisco_secret variable. **CVE ID : CVE-2023-25120**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_ike_profile function with the secrets_local variable. **CVE ID : CVE-2023-25121**	N/A	H-MIL-UR32-240723/1191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the old_remote_subnet and the old_remote_mask variables. **CVE ID : CVE-2023-25122**	N/A	H-MIL-UR32-240723/1192
Buffer Over-read	06-Jul-2023	7.5	An access violation vulnerability exists in the eventcore functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to denial of service. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2023-23571**	N/A	H-MIL-UR32-240723/1193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the remote_subnet and the remote_mask variables when action is 2. **CVE ID : CVE-2023-25123**	N/A	H-MIL-UR32-240723/1194
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow	N/A	H-MIL-UR32-240723/1195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			occurs in the set_openvpn_client function with the remote_subnet and the remote_mask variables. **CVE ID : CVE-2023-25124**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the src and dmz variables. **CVE ID : CVE-2023-25081**	N/A	H-MIL-UR32-240723/1196
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An	N/A	H-MIL-UR32-240723/1197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the old_ip and old_mac variables. **CVE ID : CVE-2023-25082**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the ip and mac variables. **CVE ID : CVE-2023-25083**	N/A	H-MIL-UR32-240723/1198
Out-of-bounds Write	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf	N/A	H-MIL-UR32-240723/1199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the ip, mac and description variables. **CVE ID : CVE-2023-25084**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the index and to_dst variables. **CVE ID : CVE-2023-25085**	N/A	H-MIL-UR32-240723/1200
Stack-based	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist	N/A	H-MIL-UR32-240723/1201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the index and dport variables. **CVE ID : CVE-2023-25086**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the index and to_dport variables.	N/A	H-MIL-UR32-240723/1202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25087		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the index and description variables. **CVE ID : CVE-2023-25088**	N/A	H-MIL-UR32-240723/1203
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This	N/A	H-MIL-UR32-240723/1204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer overflow occurs in the handle_interface_acl function with the interface variable when in_acl is -1. **CVE ID : CVE-2023-25089**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the handle_interface_acl function with the interface and in_acl variables. **CVE ID : CVE-2023-25090**	N/A	H-MIL-UR32-240723/1205
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a	N/A	H-MIL-UR32-240723/1206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the handle_interface_acl function with the interface variable when out_acl is -1. **CVE ID : CVE-2023-25091**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the handle_interface_acl function with the interface and out_acl variables. **CVE ID : CVE-2023-25092**	N/A	H-MIL-UR32-240723/1207
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due	N/A	H-MIL-UR32-240723/1208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_qos function with the class_name variable.. **CVE ID : CVE-2023-25093**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the into_class_node function with either the class_name or old_class_name variable. **CVE ID : CVE-2023-25094**	N/A	H-MIL-UR32-240723/1209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_qos function with the rule_name variable with two possible format strings that represent negated commands. **CVE ID : CVE-2023-25095**	N/A	H-MIL-UR32-240723/1210
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow	N/A	H-MIL-UR32-240723/1211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			occurs in the set_qos function with the rule_name variable with two possible format strings. **CVE ID : CVE-2023-25096**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_qos function with the source variable. **CVE ID : CVE-2023-25098**	N/A	H-MIL-UR32-240723/1212
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to	N/A	H-MIL-UR32-240723/1213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trigger these vulnerabilities.This buffer overflow occurs in the set_qos function with the dest variable. **CVE ID : CVE-2023-25099**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_qos function with the default_class variable. **CVE ID : CVE-2023-25100**	N/A	H-MIL-UR32-240723/1214
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An	N/A	H-MIL-UR32-240723/1215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_dmvpn function with the gre_key variable. **CVE ID : CVE-2023-25101**		
Out-of-bounds Write	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_dmvpn function with the hub_ip and the hub_gre_ip variables. **CVE ID : CVE-2023-25102**	N/A	H-MIL-UR32-240723/1216
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf	N/A	H-MIL-UR32-240723/1217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_dmvpn function with the gre_ip and the gre_mask variables. **CVE ID : CVE-2023-25103**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_ike_profile function with the username and the password variables. **CVE ID : CVE-2023-25104**	N/A	H-MIL-UR32-240723/1218
Stack-based	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist	N/A	H-MIL-UR32-240723/1219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_ike_profile function with the secrets_remote variable. **CVE ID : CVE-2023-25105**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_gre function with the local_virtual_ip and the	N/A	H-MIL-UR32-240723/1220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local_virtual_mask variables. **CVE ID : CVE-2023-25106**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_gre function with the remote_subnet and the remote_mask variables. **CVE ID : CVE-2023-25107**	N/A	H-MIL-UR32-240723/1221
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these	N/A	H-MIL-UR32-240723/1222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities.This buffer overflow occurs in the set_gre function with the remote_ip variable. **CVE ID : CVE-2023-25108**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_gre function with the local_ip variable. **CVE ID : CVE-2023-25109**	N/A	H-MIL-UR32-240723/1223
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to	N/A	H-MIL-UR32-240723/1224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trigger these vulnerabilities.This buffer overflow occurs in the set_gre function with the remote_virtual_ip variable. **CVE ID : CVE-2023-25110**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_gre function with the key variable. **CVE ID : CVE-2023-25111**	N/A	H-MIL-UR32-240723/1225
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An	N/A	H-MIL-UR32-240723/1226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_l2tp function with the remote_subnet and the remote_mask variables. **CVE ID : CVE-2023-25112**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_l2tp function with the key variable. **CVE ID : CVE-2023-25113**	N/A	H-MIL-UR32-240723/1227
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially	N/A	H-MIL-UR32-240723/1228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the expert_options variable. **CVE ID : CVE-2023-25114**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the remote_ip and the port variables. **CVE ID : CVE-2023-25115**	N/A	H-MIL-UR32-240723/1229
Stack-based	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus	N/A	H-MIL-UR32-240723/1230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the local_virtual_ip and the remote_virtual_ip variables. **CVE ID : CVE-2023-25116**		
Out-of-bounds Write	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the local_virtual_ip and the	N/A	H-MIL-UR32-240723/1231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local_virtual_mask variables. **CVE ID : CVE-2023-25117**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the username and the password variables. **CVE ID : CVE-2023-25118**	N/A	H-MIL-UR32-240723/1232
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jul-2023	7.2	An OS command injection vulnerability exists in the libzebra.so bridge_group functionality of Milesight UR32L v32.3.0.5. A specially crafted network packet can lead to command execution. An attacker can send a sequence of	N/A	H-MIL-UR32-240723/1233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests to trigger this vulnerability. **CVE ID : CVE-2023-22306**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jul-2023	7.2	An OS command injection vulnerability exists in the ys_thirdparty check_system_user functionality of Milesight UR32L v32.3.0.5. A specially crafted set of network packets can lead to command execution. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2023-22365**	N/A	H-MIL-UR32-240723/1234
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jul-2023	7.2	An os command injection vulnerability exists in the libzebra.so change_hostname functionality of Milesight UR32L v32.3.0.5. A specially-crafted network packets can lead to command execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2023-22659**	N/A	H-MIL-UR32-240723/1235
Improper Neutralizat	06-Jul-2023	7.2	An OS command injection	N/A	H-MIL-UR32-240723/1236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			vulnerability exists in the ys_thirdparty user_delete functionality of Milesight UR32L v32.3.0.5. A specially crafted network packet can lead to command execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2023-23550**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jul-2023	7.2	An OS command injection vulnerability exists in the ys_thirdparty system_user_script functionality of Milesight UR32L v32.3.0.5. A specially crafted series of network requests can lead to command execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2023-24595**	N/A	H-MIL-UR32-240723/1237
Improper Neutralization of Special Elements used in an OS Command ('OS	06-Jul-2023	7.2	Two OS command injection vulnerabilities exist in the zebra vlan_name functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to	N/A	H-MIL-UR32-240723/1238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			command execution. An attacker can send a network request to trigger these vulnerabilities.This command injection is in the code branch that manages an already existing vlan configuration. **CVE ID : CVE-2023-25582**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jul-2023	7.2	Two OS command injection vulnerabilities exist in the zebra vlan_name functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to command execution. An attacker can send a network request to trigger these vulnerabilities.This command injection is in the code branch that manages a new vlan configuration. **CVE ID : CVE-2023-25583**	N/A	H-MIL-UR32-240723/1239
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jul-2023	6.5	A directory traversal vulnerability exists in the luci2-io file-export mib functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to arbitrary file read.	N/A	H-MIL-UR32-240723/1240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2023-23547**		
Vendor: Moxa					
Product: tn-5900					
Affected Version(s): -					
Observable Discrepancy	05-Jul-2023	5.3	TN-5900 Series version 3.3 and prior versions is vulnearble to user enumeration vulnerability. The vulnerability may allow a remote attacker to determine whether a user is valid during password recovery through the web login page and enable a brute force attack with valid users. **CVE ID : CVE-2023-3336**	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-230401-tn-5900-series-user-enumeration-vulnerability	H-MOX-TN-5-240723/1241
Vendor: nio					
Product: ec6					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory	06-Jul-2023	7.8	An issue in the com.nextev.datastatistic component of NIO EC6 Aspen before v3.3.0 allows attackers to escalate	N/A	H-NIO-EC6-240723/1242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			privileges via path traversal. **CVE ID : CVE-2023-24256**		
Vendor: Nvidia					
Product: dgx_a100					
Affected Version(s): -					
Improper Privilege Management	04-Jul-2023	7.8	NVIDIA DGX A100/A800 contains a vulnerability in SBIOS where an attacker may cause execution with unnecessary privileges by leveraging a weakness whereby proper input parameter validation is not performed. A successful exploit of this vulnerability may lead to denial of service, information disclosure, and data tampering.	https://nvidia.custhelp.com/app/answers/detail/a_id/5461	H-NVI-DGX_-240723/1243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25521		
Improper Input Validation	04-Jul-2023	7.8	NVIDIA DGX A100/A800 contains a vulnerability in SBIOS where an attacker may cause improper input validation by providing configuration information in an unexpected format. A successful exploit of this vulnerability may lead to denial of service, information disclosure, and data tampering. **CVE ID : CVE-2023-25522**	https://nvidia.custhelp.com/app/answers/detail/a_id/5461	H-NVI-DGX_-240723/1244
Product: dgx_a800					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Privilege Management	04-Jul-2023	7.8	NVIDIA DGX A100/A800 contains a vulnerability in SBIOS where an attacker may cause execution with unnecessary privileges by leveraging a weakness whereby proper input parameter validation is not performed. A successful exploit of this vulnerability may lead to denial of service, information disclosure, and data tampering. **CVE ID : CVE-2023-25521**	https://nvidia.custhelp.com/app/answers/detail/a_id/5461	H-NVI-DGX_-240723/1245
Improper Input Validation	04-Jul-2023	7.8		https://nvidia.custhelp.com/app/answers/detail/a_id/5461	H-NVI-DGX_-240723/1246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NVIDIA DGX A100/A800 contains a vulnerability in SBIOS where an attacker may cause improper input validation by providing configuration information in an unexpected format. A successful exploit of this vulnerability may lead to denial of service, information disclosure, and data tampering. **CVE ID : CVE-2023-25522**		
Vendor: ovarro					
Product: tbox_lt2					
Affected Version(s): -					
Inclusion of Functionality from Untrusted Control Sphere	03-Jul-2023	7.2	The affected TBox RTUs run OpenVPN with root privileges and can run user defined configuration scripts.	N/A	H-OVA-TBOX-240723/1247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker could set up a local OpenVPN server and push a malicious script onto the TBox host to acquire root privileges. **CVE ID : CVE-2023-36609**		
Cleartext Storage of Sensitive Informatio n	03-Jul-2023	6.5	?All versions of the TWinSoft Configuration Tool store encrypted passwords as plaintext in memory. An attacker with access to system files could open a file to load the document into memory, including sensitive information associated with document, such as password. The attacker could then obtain the plaintext password by using a memory viewer. **CVE ID : CVE-2023-3395**	N/A	H-OVA-TBOX-240723/1248
Use of a Broken or Risky Cryptograp	03-Jul-2023	6.5	The affected TBox RTUs store hashed passwords using MD5 encryption,	N/A	H-OVA-TBOX-240723/1249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
hic Algorithm			which is an insecure encryption algorithm. **CVE ID : CVE-2023-36608**		
Improper Authorization	03-Jul-2023	6.5	The affected TBox RTUs allow low privilege users to access software security tokens of higher privilege. This could allow an attacker with "user" privileges to access files requiring higher privileges by establishing an SSH session and providing the other tokens. **CVE ID : CVE-2023-36611**	N/A	H-OVA-TBOX-240723/1250
Insufficient Entropy	03-Jul-2023	5.9	?The affected TBox RTUs generate software security tokens using insufficient entropy. The random seed used to generate the software tokens is not initialized correctly, and other parts of the token are generated using predictable time-based values. An attacker with this	N/A	H-OVA-TBOX-240723/1251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			knowledge could successfully brute force the token and authenticate themselves. **CVE ID : CVE-2023-36610**		
Product: tbox_ms-cpu32					
Affected Version(s): -					
Inclusion of Functionality from Untrusted Control Sphere	03-Jul-2023	7.2	The affected TBox RTUs run OpenVPN with root privileges and can run user defined configuration scripts. An attacker could set up a local OpenVPN server and push a malicious script onto the TBox host to acquire root privileges. **CVE ID : CVE-2023-36609**	N/A	H-OVA-TBOX-240723/1252
Cleartext Storage of Sensitive Information	03-Jul-2023	6.5	?All versions of the TWinSoft Configuration Tool store encrypted passwords as plaintext in memory. An attacker with access to system files could open a file to load the document	N/A	H-OVA-TBOX-240723/1253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			into memory, including sensitive information associated with document, such as password. The attacker could then obtain the plaintext password by using a memory viewer. **CVE ID : CVE-2023-3395**		
Use of a Broken or Risky Cryptographic Algorithm	03-Jul-2023	6.5	The affected TBox RTUs store hashed passwords using MD5 encryption, which is an insecure encryption algorithm. **CVE ID : CVE-2023-36608**	N/A	H-OVA-TBOX-240723/1254
Improper Authorization	03-Jul-2023	6.5	The affected TBox RTUs allow low privilege users to access software security tokens of higher privilege. This could allow an attacker with “user” privileges to access files requiring higher privileges by establishing an SSH session and providing the other tokens.	N/A	H-OVA-TBOX-240723/1255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36611		
Insufficient Entropy	03-Jul-2023	5.9	?The affected TBox RTUs generate software security tokens using insufficient entropy. The random seed used to generate the software tokens is not initialized correctly, and other parts of the token are generated using predictable time-based values. An attacker with this knowledge could successfully brute force the token and authenticate themselves. **CVE ID : CVE-2023-36610**	N/A	H-OVA-TBOX-240723/1256
Product: tbox_ms-cpu32-s2					
Affected Version(s): -					
Inclusion of Functionality from Untrusted Control Sphere	03-Jul-2023	7.2	The affected TBox RTUs run OpenVPN with root privileges and can run user defined configuration scripts. An attacker could set up a local OpenVPN server and push a malicious script onto	N/A	H-OVA-TBOX-240723/1257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the TBox host to acquire root privileges. **CVE ID : CVE-2023-36609**		
Cleartext Storage of Sensitive Information	03-Jul-2023	6.5	?All versions of the TWinSoft Configuration Tool store encrypted passwords as plaintext in memory. An attacker with access to system files could open a file to load the document into memory, including sensitive information associated with document, such as password. The attacker could then obtain the plaintext password by using a memory viewer. **CVE ID : CVE-2023-3395**	N/A	H-OVA-TBOX-240723/1258
Use of a Broken or Risky Cryptographic Algorithm	03-Jul-2023	6.5	The affected TBox RTUs store hashed passwords using MD5 encryption, which is an insecure encryption algorithm.	N/A	H-OVA-TBOX-240723/1259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36608		
Improper Authorization	03-Jul-2023	6.5	The affected TBox RTUs allow low privilege users to access software security tokens of higher privilege. This could allow an attacker with "user" privileges to access files requiring higher privileges by establishing an SSH session and providing the other tokens. **CVE ID : CVE-2023-36611**	N/A	H-OVA-TBOX-240723/1260
Insufficient Entropy	03-Jul-2023	5.9	?The affected TBox RTUs generate software security tokens using insufficient entropy. The random seed used to generate the software tokens is not initialized correctly, and other parts of the token are generated using predictable time-based values. An attacker with this knowledge could successfully brute force the token and	N/A	H-OVA-TBOX-240723/1261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticate themselves. **CVE ID : CVE-2023-36610**		
Product: tbox_rm2					
Affected Version(s): -					
Inclusion of Functionality from Untrusted Control Sphere	03-Jul-2023	7.2	The affected TBox RTUs run OpenVPN with root privileges and can run user defined configuration scripts. An attacker could set up a local OpenVPN server and push a malicious script onto the TBox host to acquire root privileges. **CVE ID : CVE-2023-36609**	N/A	H-OVA-TBOX-240723/1262
Cleartext Storage of Sensitive Information	03-Jul-2023	6.5	?All versions of the TWinSoft Configuration Tool store encrypted passwords as plaintext in memory. An attacker with access to system files could open a file to load the document into memory, including sensitive information	N/A	H-OVA-TBOX-240723/1263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			associated with document, such as password. The attacker could then obtain the plaintext password by using a memory viewer. **CVE ID : CVE-2023-3395**		
Use of a Broken or Risky Cryptographic Algorithm	03-Jul-2023	6.5	The affected TBox RTUs store hashed passwords using MD5 encryption, which is an insecure encryption algorithm. **CVE ID : CVE-2023-36608**	N/A	H-OVA-TBOX-240723/1264
Improper Authorization	03-Jul-2023	6.5	The affected TBox RTUs allow low privilege users to access software security tokens of higher privilege. This could allow an attacker with “user” privileges to access files requiring higher privileges by establishing an SSH session and providing the other tokens.	N/A	H-OVA-TBOX-240723/1265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36611		
Insufficient Entropy	03-Jul-2023	5.9	?The affected TBox RTUs generate software security tokens using insufficient entropy. The random seed used to generate the software tokens is not initialized correctly, and other parts of the token are generated using predictable time-based values. An attacker with this knowledge could successfully brute force the token and authenticate themselves. **CVE ID : CVE-2023-36610**	N/A	H-OVA-TBOX-240723/1266
Product: tbox_tg2					
Affected Version(s): -					
Inclusion of Functionality from Untrusted Control Sphere	03-Jul-2023	7.2	The affected TBox RTUs run OpenVPN with root privileges and can run user defined configuration scripts. An attacker could set up a local OpenVPN server and push a malicious script onto the TBox host to	N/A	H-OVA-TBOX-240723/1267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			acquire root privileges. **CVE ID : CVE-2023-36609**		
Cleartext Storage of Sensitive Information	03-Jul-2023	6.5	?All versions of the TWinSoft Configuration Tool store encrypted passwords as plaintext in memory. An attacker with access to system files could open a file to load the document into memory, including sensitive information associated with document, such as password. The attacker could then obtain the plaintext password by using a memory viewer. **CVE ID : CVE-2023-3395**	N/A	H-OVA-TBOX-240723/1268
Use of a Broken or Risky Cryptographic Algorithm	03-Jul-2023	6.5	The affected TBox RTUs store hashed passwords using MD5 encryption, which is an insecure encryption algorithm.	N/A	H-OVA-TBOX-240723/1269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36608		
Improper Authorization	03-Jul-2023	6.5	The affected TBox RTUs allow low privilege users to access software security tokens of higher privilege. This could allow an attacker with "user" privileges to access files requiring higher privileges by establishing an SSH session and providing the other tokens. **CVE ID : CVE-2023-36611**	N/A	H-OVA-TBOX-240723/1270
Insufficient Entropy	03-Jul-2023	5.9	?The affected TBox RTUs generate software security tokens using insufficient entropy. The random seed used to generate the software tokens is not initialized correctly, and other parts of the token are generated using predictable time-based values. An attacker with this knowledge could successfully brute force the token and	N/A	H-OVA-TBOX-240723/1271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticate themselves. **CVE ID : CVE-2023-36610**		
Vendor: paxtechnology					
Product: pax_a930					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Jul-2023	6.8	PAX A930 device with PayDroid_7.1.1_Virgo_V04.5.02_20220722 can allow the execution of arbitrary commands by using the exec service and including a specific word in the command to be executed. The attacker must have physical USB access to the device in order to exploit this vulnerability. **CVE ID : CVE-2023-27198**	N/A	H-PAX-PAX_-240723/1272
N/A	05-Jul-2023	6.7	PAX A930 device with PayDroid_7.1.1_Virgo_V04.5.02_20220722 can allow an attacker to gain root access by running a crafted binary leveraging an exported function from a shared library. The attacker must have shell access to the device	N/A	H-PAX-PAX_-240723/1273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in order to exploit this vulnerability. **CVE ID : CVE-2023-27197**		
N/A	05-Jul-2023	6.7	PAX Technology A930 PayDroid_7.1.1_Virgo_V04.5.02_20220722 allows attackers to compile a malicious shared library and use LD_PRELOAD to bypass authorization checks. **CVE ID : CVE-2023-27199**	N/A	H-PAX-PAX_-240723/1274
Vendor: piigab					
Product: m-bus_900s					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Jul-2023	9.8	The number of login attempts is not limited. This could allow an attacker to perform a brute force on HTTP basic authentication. **CVE ID : CVE-2023-33868**	N/A	H-PII-M-BU-240723/1275
Use of Password Hash With Insufficient	07-Jul-2023	9.8		N/A	H-PII-M-BU-240723/1276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Computational Effort			PiiGAB M-Bus stores passwords using a weak hash algorithm. **CVE ID : CVE-2023-34433**		
Weak Password Requirements	07-Jul-2023	9.8	There are no requirements for setting a complex	N/A	H-PII-M-BU-240723/1277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password for PiiGAB M-Bus, which could contribute to a successful brute force attack if the password is inline with recommended password guidelines. **CVE ID : CVE-2023-34995**		
Use of Hard-coded Credentials	06-Jul-2023	9.8	PiiGAB M-Bus contains hard-coded credentials which it uses for authentication. **CVE ID : CVE-2023-35987**	N/A	H-PII-M-BU-240723/1278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	06-Jul-2023	9.8	PiiGAB M-Bus SoftwarePack 900S does not correctly sanitize user input, which could allow an attacker to inject arbitrary commands. **CVE ID : CVE-2023-36859**	N/A	H-PII-M-BU-240723/1279
Cross-Site Request Forgery (CSRF)	07-Jul-2023	8.8	PiiGAB M-Bus is vulnerable to cross-site request forgery. An attacker who wants to execute a certain command could send a phishing mail to the owner of the device and hope that the owner clicks on the link. If the owner of the device has a cookie stored that allows the owner to be logged in, then the device could execute the GET or POST link request. **CVE ID : CVE-2023-35120**	N/A	H-PII-M-BU-240723/1280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unprotected Transport of Credentials	06-Jul-2023	7.5	PiiGAB M-Bus transmits credentials in plaintext format. **CVE ID : CVE-2023-31277**	N/A	H-PII-M-BU-240723/1281
Unprotected Storage of Credentials	07-Jul-2023	6.5	PiiGAB M-Bus stores credentials in a plaintext file, which could allow a low-level user to gain admin credentials.	N/A	H-PII-M-BU-240723/1282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35765		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	6.1	PiiGAB M-Bus does not validate identification strings before processing, which could make it vulnerable to cross-site scripting attacks.	N/A	H-PII-M-BU-240723/1283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32652		
Vendor: Qualcomm					
Product: 205					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-205-240723/1284
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-205-240723/1285
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-205-240723/1286
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-205-240723/1287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 215					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-215-240723/1288
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-215-240723/1289
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-215-240723/1290
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-215-240723/1291
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN	https://www.qualcomm.com/company/product-security/bull	H-QUA-215-240723/1292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firmware response message. **CVE ID : CVE-2023-24854**	etins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-215-240723/1293
Product: 315_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-315_-240723/1294
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-315_-240723/1295
Product: 315_5g_iot					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-315_-240723/1296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-315_-240723/1297
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-315_-240723/1298
Product: 9205					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-9205-240723/1299
Product: apq8017					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-APQ8-240723/1300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received from network. **CVE ID : CVE-2023-21631**		
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-APQ8-240723/1301
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-APQ8-240723/1302
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-APQ8-240723/1303
Product: apq8037					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-APQ8-240723/1304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-APQ8-240723/1305
Product: apq8064au					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-APQ8-240723/1306
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-APQ8-240723/1307
Product: aqt1000					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AQT1-240723/1308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AQT1-240723/1309
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AQT1-240723/1310
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AQT1-240723/1311
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AQT1-240723/1312
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AQT1-240723/1313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AQT1-240723/1314
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AQT1-240723/1315
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AQT1-240723/1316
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AQT1-240723/1317
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AQT1-240723/1318
Product: ar8031					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AR80-240723/1319
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AR80-240723/1320
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AR80-240723/1321
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AR80-240723/1322
Product: ar8035					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AR80-240723/1323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received from network. **CVE ID : CVE-2023-21631**		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AR80-240723/1324
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AR80-240723/1325
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AR80-240723/1326
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AR80-240723/1327
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-AR80-240723/1328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24854	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AR80-240723/1329
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AR80-240723/1330
Product: ar9380					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AR93-240723/1331
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-AR93-240723/1332
Product: c-v2x_9150					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in	https://www.qualcomm.com/compa	H-QUA-C-V2-240723/1333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	ny/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-C-V2-240723/1334
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-C-V2-240723/1335
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-C-V2-240723/1336
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-C-V2-240723/1337
Product: csr8811					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSR8-240723/1338
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSR8-240723/1339
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSR8-240723/1340
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSR8-240723/1341
Product: csra6620					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-CSRA-240723/1342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received from network. **CVE ID : CVE-2023-21631**	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRA-240723/1343
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRA-240723/1344
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRA-240723/1345
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRA-240723/1346
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-CSRA-240723/1347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24854	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRA-240723/1348
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRA-240723/1349
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRA-240723/1350
Product: csra6640					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRA-240723/1351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRA-240723/1352
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRA-240723/1353
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRA-240723/1354
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRA-240723/1355
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRA-240723/1356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRA-240723/1357
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRA-240723/1358
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRA-240723/1359
Product: csrb31024					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRB-240723/1360
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets	https://www.qualcomm.com/company/product-security/bull	H-QUA-CSRB-240723/1361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			detected on telephony. **CVE ID : CVE-2023-21635**	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRB-240723/1362
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRB-240723/1363
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRB-240723/1364
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-CSRB-240723/1365
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-CSRB-240723/1366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
Product: fastconnect_6200					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1367
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1368
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1369
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1371
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1372
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1373
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1374
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1376
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1377
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1378
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1379
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1380
Product: fastconnect_6700					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1381
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1382
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1383
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1384
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-FAST-240723/1385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1386
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1387
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1388
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1389
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1391
Product: fastconnect_6800					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1392
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1393
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1394
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs.	https://www.qualcomm.com/company/product-	H-QUA-FAST-240723/1395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21637	security/bulletins/july-2023-bulletin	
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1396
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1397
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1398
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1399
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-FAST-240723/1400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24851	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1401
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1402
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1403
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1404
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: fastconnect_6900					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1406
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1407
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1408
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1409
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the	https://www.qualcomm.com/company/product-	H-QUA-FAST-240723/1410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			one received in initialization. **CVE ID : CVE-2023-21638**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux when the file upload API is called with parameters having large buffer. **CVE ID : CVE-2023-21640**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1411
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1412
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1413
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1414
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/company/product-	H-QUA-FAST-240723/1415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	security/bulletins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1416
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1417
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1418
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1419
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-FAST-240723/1420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1421
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1422
Product: fastconnect_7800					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1423
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux when the file upload API is called with parameters having large buffer. **CVE ID : CVE-2023-21640**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1425
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1426
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1427
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1428
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1430
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1431
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1432
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1433
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FAST-240723/1434
Product: flight_rb5_5g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FLIG-240723/1435
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FLIG-240723/1436
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FLIG-240723/1437
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FLIG-240723/1438
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FLIG-240723/1439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FLIG-240723/1440
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-FLIG-240723/1441
Product: home_hub_100					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-HOME-240723/1442
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-HOME-240723/1443
Product: immersive_home_214					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	https://www.qualcomm.com/company/product-security/bull	H-QUA-IMME-240723/1444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22386	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IMME-240723/1445
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IMME-240723/1446
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IMME-240723/1447
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IMME-240723/1448
Product: immersive_home_216					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/company/product-security/bull	H-QUA-IMME-240723/1449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IMME-240723/1450
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IMME-240723/1451
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IMME-240723/1452
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IMME-240723/1453
Product: immersive_home_316					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/compa	H-QUA-IMME-240723/1454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	ny/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IMME-240723/1455
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IMME-240723/1456
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IMME-240723/1457
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IMME-240723/1458
Product: immersive_home_318					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IMME-240723/1459
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IMME-240723/1460
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IMME-240723/1461
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IMME-240723/1462
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IMME-240723/1463
Product: ipq4018					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ4-240723/1464
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ4-240723/1465
Product: ipq4019					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ4-240723/1466
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ4-240723/1467
Product: ipq4028					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ4-240723/1468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ4-240723/1469
Product: ipq4029					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ4-240723/1470
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ4-240723/1471
Product: ipq5010					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ5-240723/1472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ5-240723/1473
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ5-240723/1474
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ5-240723/1475
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ5-240723/1476
Product: ipq5028					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ5-240723/1477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ5-240723/1478
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ5-240723/1479
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ5-240723/1480
Product: ipq6000					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ6-240723/1481
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ6-240723/1482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ6-240723/1483
Product: ipq6010					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ6-240723/1484
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ6-240723/1485
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ6-240723/1486
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ6-240723/1487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ipq6018					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ6-240723/1488
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ6-240723/1489
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ6-240723/1490
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ6-240723/1491
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ6-240723/1492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ipq6028					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ6-240723/1493
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ6-240723/1494
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ6-240723/1495
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ6-240723/1496
Product: ipq8064					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ8-240723/1497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1498
Product: ipq8065					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1499
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1500
Product: ipq8068					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1502
Product: ipq8070					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1503
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1504
Product: ipq8070a					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1505
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ8-240723/1506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1507
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1508
Product: ipq8071a					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1509
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1510
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ8-240723/1511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1512
Product: ipq8072a					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1513
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1514
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1515
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA	https://www.qualcomm.com/compa	H-QUA-IPQ8-240723/1516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer release event about CFR data. **CVE ID : CVE-2023-28541**	ny/product-security/bulletins/july-2023-bulletin	
Product: ipq8074a					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1517
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1518
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1519
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1521
Product: ipq8076					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1522
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1523
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1524
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ipq8076a					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1526
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1527
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1528
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1529
Product: ipq8078					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ8-240723/1530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22386	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1531
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1532
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1533
Product: ipq8078a					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1534
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ8-240723/1535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1536
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1537
Product: ipq8173					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1538
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1539
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/compa	H-QUA-IPQ8-240723/1540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1541
Product: ipq8174					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1542
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1543
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1545
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ8-240723/1546
Product: ipq9008					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ9-240723/1547
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ9-240723/1548
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ9-240723/1549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ipq9574					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ9-240723/1550
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ9-240723/1551
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ9-240723/1552
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-IPQ9-240723/1553
Product: mdm9250					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bull	H-QUA-MDM9-240723/1554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MDM9-240723/1555
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MDM9-240723/1556
Product: mdm9628					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MDM9-240723/1557
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MDM9-240723/1558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MDM9-240723/1559
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MDM9-240723/1560
Product: mdm9640					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MDM9-240723/1561
Product: mdm9650					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MDM9-240723/1562
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bull	H-QUA-MDM9-240723/1563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	etins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MDM9-240723/1564
Product: msm8108					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MSM8-240723/1565
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MSM8-240723/1566
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MSM8-240723/1567
Product: msm8209					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MSM8-240723/1568
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MSM8-240723/1569
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MSM8-240723/1570
Product: msm8608					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MSM8-240723/1571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MSM8-240723/1572
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MSM8-240723/1573
Product: msm8909w					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MSM8-240723/1574
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MSM8-240723/1575
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while	https://www.qualcomm.com/company/product-security/bull	H-QUA-MSM8-240723/1576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	etins/july-2023-bulletin	
Product: msm8996au					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MSM8-240723/1577
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MSM8-240723/1578
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-MSM8-240723/1579
Product: pmp8074					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-PMP8-240723/1580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qam8255p					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1581
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1582
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1583
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1584
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QAM8-240723/1585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24851	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1586
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1587
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1588
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1589
Product: qam8295p					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsReg	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QAM8-240723/1590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			isterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	2023-bulletin	
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1591
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1592
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1593
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1594
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/company/product-security/bull	H-QUA-QAM8-240723/1595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1596
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1597
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1598
Product: qam8650p					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1600
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1601
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1602
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1603
Product: qam8775p					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21672		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1605
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1606
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1607
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QAM8-240723/1608
Product: qca4004					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA4-240723/1609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command message received from network. **CVE ID : CVE-2023-21631**	2023-bulletin	
Product: qca4024					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA4-240723/1610
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA4-240723/1611
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA4-240723/1612
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA4-240723/1613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA4-240723/1614
Product: qca6174a					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1615
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1616
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1617
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-240723/1618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1619
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1620
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1621
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1622
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-240723/1623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
Product: qca6175a					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1624
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1625
Product: qca6310					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1626
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1627
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/compa	H-QUA-QCA6-240723/1628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1629
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1630
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1631
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1632
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-240723/1633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	etins/july-2023-bulletin	
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1634
Product: qca6320					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1635
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1636
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1637
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-240723/1638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firmware response message. **CVE ID : CVE-2023-24854**	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1639
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1640
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1641
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1642
Product: qca6335					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/compa	H-QUA-QCA6-240723/1643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	ny/product-security/bulletins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1644
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1645
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1646
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1647
Product: qca6391					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in	https://www.qualcomm.com/compa	H-QUA-QCA6-240723/1648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1649
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1650
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1651
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1653
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1654
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1655
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1656
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1658
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1659
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1660
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1661
Product: qca6420					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received from network. **CVE ID : CVE-2023-21631**		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1663
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1664
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1665
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1666
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-240723/1667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed by HIDL client. **CVE ID : CVE-2023-21639**	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1668
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1669
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1670
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1671
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-240723/1672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
Product: qca6421					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1673
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1674
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1675
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1676
Integer Overflow	04-Jul-2023	7.8	Memory Corruption in Audio while	https://www.qualcomm	H-QUA-QCA6-240723/1677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	.com/company/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1678
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1679
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1680
Product: qca6426					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21631		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1682
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1683
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1684
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1685
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-240723/1686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1687
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1688
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1689
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1690
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1692
Product: qca6430					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1693
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1694
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1695
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs.	https://www.qualcomm.com/company/product-	H-QUA-QCA6-240723/1696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21637	security/bulletins/july-2023-bulletin	
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1697
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1698
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1699
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1700
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-240723/1701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer release event about CFR data. **CVE ID : CVE-2023-28541**	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1702
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1703
Product: qca6431					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1704
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1706
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1707
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1708
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1709
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1710
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to	https://www.qualcomm	H-QUA-QCA6-240723/1711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: qca6436					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1712
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1713
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1714
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-240723/1715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21637	2023-bulletin	
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1716
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1717
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1718
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1719
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1721
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1722
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1723
Product: qca6554a					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1724
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1726
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1727
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1728
Product: qca6564					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1729
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-240723/1730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21635	2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1731
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1732
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1733
Product: qca6564a					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1735
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1736
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1737
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1738
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1739
Product: qca6564au					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1740
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1741
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1742
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1743
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-240723/1744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	etins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1745
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1746
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1747
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1748
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-240723/1749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1750
Product: qca6574					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1751
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1752
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1753
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/company/product-	H-QUA-QCA6-240723/1754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	security/bulletins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1755
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1756
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1757
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1758
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-240723/1759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	2023-bulletin	
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1760
Product: qca6574a					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1761
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1762
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1764
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1765
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1766
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1767
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1769
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1770
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1771
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1772
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1773
N/A	04-Jul-2023	5.5	Information disclosure in DSP	https://www.qualcomm	H-QUA-QCA6-240723/1774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Services while loading dynamic module. **CVE ID : CVE-2023-21624**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: qca6574au					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1775
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1776
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1777
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-240723/1778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21637	2023-bulletin	
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1779
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1780
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1781
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1782
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-240723/1783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1784
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1785
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1786
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1787
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1789
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1790
Product: qca6584					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1791
Product: qca6584au					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1792
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-240723/1793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1794
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1795
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1796
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1797
Product: qca6595					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsReg	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-240723/1798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			isterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	etins/july-2023-bulletin	
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1799
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1800
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1801
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1802
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-240723/1803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1804
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1805
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1806
Product: qca6595au					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1808
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1809
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1810
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1811
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1813
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1814
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1815
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1816
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1818
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1819
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1820
Product: qca6678aq					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1821
Product: qca6696					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-240723/1822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security mode command message received from network. **CVE ID : CVE-2023-21631**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1823
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1824
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1825
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1826
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system	https://www.qualcomm.com/compa	H-QUA-QCA6-240723/1827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	ny/product-security/bulletins/july-2023-bulletin	
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1828
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1829
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1830
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1831
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/company/product-	H-QUA-QCA6-240723/1832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1833
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1834
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1835
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1836
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-240723/1837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21624	2023-bulletin	
Product: qca6698aq					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1838
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1839
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1840
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1842
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1843
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1844
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1845
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1847
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1848
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1849
Product: qca6797aq					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1850
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-240723/1851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22386	2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1852
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1853
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1854
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1855
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1857
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA6-240723/1858
Product: qca7500					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA7-240723/1859
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA7-240723/1860
Product: qca8072					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA8-240723/1861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22386	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1862
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1863
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1864
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1865
Product: qca8075					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA8-240723/1866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1867
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1868
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1869
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1870
Product: qca8081					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in	https://www.qualcomm.com/compa	H-QUA-QCA8-240723/1871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1872
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1873
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1874
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1876
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1877
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1878
Product: qca8082					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1879
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1881
Product: qca8084					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1882
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1883
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1884
Product: qca8085					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA8-240723/1885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22386	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1886
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1887
Product: qca8337					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1888
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1890
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1891
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1892
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1893
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1895
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1896
Product: qca8386					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1897
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1898
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA8-240723/1899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca9367					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1900
Product: qca9377					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1901
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1902
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1903
Integer Overflow	04-Jul-2023	7.8	Memory Corruption in Audio while	https://www.qualcomm	H-QUA-QCA9-240723/1904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	.com/company/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1905
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1906
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1907
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1908
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while	https://www.qualcomm.com/company/product-	H-QUA-QCA9-240723/1909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	security/bulletins/july-2023-bulletin	
Product: qca9379					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1910
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1911
Product: qca9880					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1912
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca9886					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1914
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1915
Product: qca9888					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1916
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1917
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA9-240723/1918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24851	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1919
Product: qca9889					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1920
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1921
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1922
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA9-240723/1923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer release event about CFR data. **CVE ID : CVE-2023-28541**	etins/july-2023-bulletin	
Product: qca9898					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1924
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1925
Product: qca9980					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1926
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca9984					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1928
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1929
Product: qca9985					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1930
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1931
Product: qca9986					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM	https://www.qualcomm	H-QUA-QCA9-240723/1932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: qca9990					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1933
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1934
Product: qca9992					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1935
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA9-240723/1936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: qca9994					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1937
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCA9-240723/1938
Product: qcm2290					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM2-240723/1939
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM2-240723/1940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM2-240723/1941
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM2-240723/1942
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM2-240723/1943
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM2-240723/1944
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM2-240723/1945
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to	https://www.qualcomm	H-QUA-QCM2-240723/1946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: qcm4290					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM4-240723/1947
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM4-240723/1948
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM4-240723/1949
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCM4-240723/1950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM4-240723/1951
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM4-240723/1952
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM4-240723/1953
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM4-240723/1954
Product: qcm4325					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCM4-240723/1955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command message received from network. **CVE ID : CVE-2023-21631**	2023-bulletin	
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM4-240723/1956
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM4-240723/1957
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM4-240723/1958
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM4-240723/1959
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN	https://www.qualcomm.com/company/product-	H-QUA-QCM4-240723/1960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firmware response message. **CVE ID : CVE-2023-24854**	security/bulletins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM4-240723/1961
Product: qcm4490					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM4-240723/1962
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM4-240723/1963
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM4-240723/1964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM4-240723/1965
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM4-240723/1966
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM4-240723/1967
Product: qcm6125					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM6-240723/1968
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM6-240723/1969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM6-240723/1970
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM6-240723/1971
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM6-240723/1972
Product: qcm6490					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM6-240723/1973
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCM6-240723/1974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM6-240723/1975
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM6-240723/1976
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM6-240723/1977
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM6-240723/1978
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCM6-240723/1979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM6-240723/1980
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCM6-240723/1981
Product: qcn5021					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/1982
Product: qcn5022					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/1983
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/compa	H-QUA-QCN5-240723/1984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/1985
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/1986
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/1987
Product: qcn5024					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/1988
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/compa	H-QUA-QCN5-240723/1989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/1990
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/1991
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/1992
Product: qcn5052					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/1993
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/compa	H-QUA-QCN5-240723/1994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/1995
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/1996
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/1997
Product: qcn5054					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/1998
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/compa	H-QUA-QCN5-240723/1999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2000
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2001
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2002
Product: qcn5122					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2003
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/compa	H-QUA-QCN5-240723/2004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2005
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2006
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2007
Product: qcn5124					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2008
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/compa	H-QUA-QCN5-240723/2009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2010
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2011
Product: qcn5152					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2012
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2014
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2015
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2016
Product: qcn5154					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2017
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2019
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2020
Product: qcn5164					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2021
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2022
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN5-240723/2024
Product: qcn6023					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2025
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2026
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2027
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcn6024					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2029
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2030
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2031
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2032
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCN6-240723/2033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firmware response message. **CVE ID : CVE-2023-24854**	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2034
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2035
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2036
Product: qcn6100					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2037
Product: qcn6102					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2038
Product: qcn6112					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2039
Product: qcn6122					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2040
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2041
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCN6-240723/2042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24851	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2043
Product: qcn6132					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2044
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2045
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN6-240723/2046
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCN6-240723/2047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer release event about CFR data. **CVE ID : CVE-2023-28541**	etins/july-2023-bulletin	
Product: qcn7605					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN7-240723/2048
Product: qcn7606					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN7-240723/2049
Product: qcn9000					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2050
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCN9-240723/2051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2052
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2053
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2054
Product: qcn9001					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2055
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCN9-240723/2056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24851	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2057
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2058
Product: qcn9002					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2059
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2060
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCN9-240723/2061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24854	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2062
Product: qcn9003					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2063
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2064
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2065
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCN9-240723/2066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	2023-bulletin	
Product: qcn9011					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2067
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2068
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2069
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2070
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCN9-240723/2071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24854	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2072
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2073
Product: qcn9012					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2074
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2075
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCN9-240723/2076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2077
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2078
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2079
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2080
Product: qcn9022					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCN9-240723/2081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22386	2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2082
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2083
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2084
Product: qcn9024					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2086
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2087
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2088
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2089
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2091
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2092
Product: qcn9070					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2093
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2094
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2096
Product: qcn9072					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2097
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2098
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2099
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcn9074					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2101
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2102
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2103
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2104
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2106
Product: qcn9100					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2107
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2108
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2109
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcn9274					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2111
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2112
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2113
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCN9-240723/2114
Product: qcs2290					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCS2-240723/2115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security mode command message received from network. **CVE ID : CVE-2023-21631**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS2-240723/2116
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS2-240723/2117
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS2-240723/2118
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS2-240723/2119
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN	https://www.qualcomm.com/company/product-	H-QUA-QCS2-240723/2120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firmware response message. **CVE ID : CVE-2023-24854**	security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS2-240723/2121
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS2-240723/2122
Product: qcs410					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS4-240723/2123
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS4-240723/2124
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/compa	H-QUA-QCS4-240723/2125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS4-240723/2126
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS4-240723/2127
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS4-240723/2128
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS4-240723/2129
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCS4-240723/2130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	etins/july-2023-bulletin	
Product: qcs4290					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS4-240723/2131
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS4-240723/2132
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS4-240723/2133
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS4-240723/2134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS4-240723/2135
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS4-240723/2136
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS4-240723/2137
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS4-240723/2138
Product: qcs4490					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS4-240723/2139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received from network. **CVE ID : CVE-2023-21631**		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS4-240723/2140
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS4-240723/2141
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS4-240723/2142
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS4-240723/2143
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCS4-240723/2144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
Product: qcs610					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2145
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2146
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2147
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2148
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCS6-240723/2149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24851	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2150
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2151
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2152
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2153
Product: qcs6125					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCS6-240723/2154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	etins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2155
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2156
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2157
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2158
Product: qcs6490					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in	https://www.qualcomm.com/compa	H-QUA-QCS6-240723/2159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2160
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2161
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2162
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2164
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2165
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2166
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS6-240723/2167
Product: qcs8155					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS8-240723/2168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS8-240723/2169
Product: qcs8250					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS8-240723/2170
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS8-240723/2171
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS8-240723/2172
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS8-240723/2173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcs8550					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS8-240723/2174
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QCS8-240723/2175
Product: qrb5165m					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QRB5-240723/2176
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QRB5-240723/2177
Integer Overflow	04-Jul-2023	7.8	Memory Corruption in Audio while	https://www.qualcomm	H-QUA-QRB5-240723/2178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	.com/company/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QRB5-240723/2179
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QRB5-240723/2180
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QRB5-240723/2181
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QRB5-240723/2182
Product: qrb5165n					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QRB5-240723/2183
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QRB5-240723/2184
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QRB5-240723/2185
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QRB5-240723/2186
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QRB5-240723/2187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QRB5-240723/2188
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QRB5-240723/2189
Product: qsm8250					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QSM8-240723/2190
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QSM8-240723/2191
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QSM8-240723/2192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qsm8350					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QSM8-240723/2193
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QSM8-240723/2194
Product: qts110					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-QTS1-240723/2195
Product: robotics_rb3					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-ROBO-240723/2196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-ROBO-240723/2197
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-ROBO-240723/2198
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-ROBO-240723/2199
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-ROBO-240723/2200
Product: robotics_rb5					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-ROBO-240723/2201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22386	2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-ROBO-240723/2202
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-ROBO-240723/2203
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-ROBO-240723/2204
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-ROBO-240723/2205
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-ROBO-240723/2206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-ROBO-240723/2207
Product: sa4150p					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA41-240723/2208
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA41-240723/2209
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA41-240723/2210
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA41-240723/2211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	etins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA41-240723/2212
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA41-240723/2213
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA41-240723/2214
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA41-240723/2215
Product: sa4155p					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA41-240723/2216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed by HIDL client. **CVE ID : CVE-2023-21639**	etins/july-2023-bulletin	
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA41-240723/2217
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA41-240723/2218
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA41-240723/2219
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA41-240723/2220
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA41-240723/2221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA41-240723/2222
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA41-240723/2223
Product: sa6145p					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2224
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2226
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2227
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2228
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2229
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2231
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2232
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2233
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2234
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2236
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2237
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2238
Product: sa6150p					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2239
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SA61-240723/2240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21635	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2241
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2242
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2243
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2244
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SA61-240723/2245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22386	2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2246
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2247
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2248
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2249
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2251
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2252
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2253
Product: sa6155					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2254
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SA61-240723/2255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2256
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2257
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2258
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2259
Product: sa6155p					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsReg	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SA61-240723/2260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			isterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2261
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2262
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2263
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2264
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause	https://www.qualcomm.com/company/product-	H-QUA-SA61-240723/2265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undesired system behavior. **CVE ID : CVE-2023-21641**	security/bulletins/july-2023-bulletin	
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2266
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2267
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2268
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2269
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA61-240723/2270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2271
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2272
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2273
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA61-240723/2274
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SA61-240723/2275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21624	2023-bulletin	
Product: sa8145p					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2276
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2277
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2278
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2279
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA81-240723/2280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undesired system behavior. **CVE ID : CVE-2023-21641**	etins/july-2023-bulletin	
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2281
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2282
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2283
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2284
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA81-240723/2285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2286
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2287
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2288
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2289
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SA81-240723/2290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21624	2023-bulletin	
Product: sa8150p					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2291
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2292
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2293
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2294
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA81-240723/2295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undesired system behavior. **CVE ID : CVE-2023-21641**	etins/july-2023-bulletin	
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2296
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2297
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2298
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2299
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA81-240723/2300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2301
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2302
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2303
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2304
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SA81-240723/2305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21624	2023-bulletin	
Product: sa8155					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2306
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2307
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2308
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2309
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA81-240723/2310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	etins/july-2023-bulletin	
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2311
Product: sa8155p					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2312
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2313
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2314
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the	https://www.qualcomm.com/company/product-	H-QUA-SA81-240723/2315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			one received in initialization. **CVE ID : CVE-2023-21638**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2316
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2317
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2318
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2319
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/compa	H-QUA-SA81-240723/2320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	ny/product-security/bulletins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2321
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2322
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2323
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2324
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA81-240723/2325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	etins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2326
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2327
Product: sa8195p					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2328
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2329
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs.	https://www.qualcomm.com/company/product-	H-QUA-SA81-240723/2330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21637	security/bulletins/july-2023-bulletin	
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2331
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2332
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2333
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2334
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/compa	H-QUA-SA81-240723/2335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	ny/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2336
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2337
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2338
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2339
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA81-240723/2340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2341
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2342
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA81-240723/2343
Product: sa8255p					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA82-240723/2344
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/compa	H-QUA-SA82-240723/2345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	ny/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA82-240723/2346
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA82-240723/2347
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA82-240723/2348
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA82-240723/2349
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA82-240723/2350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA82-240723/2351
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA82-240723/2352
Product: sa8295p					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA82-240723/2353
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA82-240723/2354
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/compa	H-QUA-SA82-240723/2355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	ny/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA82-240723/2356
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA82-240723/2357
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA82-240723/2358
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA82-240723/2359
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA82-240723/2360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SA82-240723/2361
Product: sc8180x-aa					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SC81-240723/2362
Product: sc8180x-aaab					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SC81-240723/2363
Product: sc8180x-ab					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while	https://www.qualcomm.com/company/product-	H-QUA-SC81-240723/2364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	security/bulletins/july-2023-bulletin	
Product: sc8180x-ac					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SC81-240723/2365
Product: sc8180x-acaf					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SC81-240723/2366
Product: sc8180x-ad					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SC81-240723/2367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received from network. **CVE ID : CVE-2023-21631**		
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SC81-240723/2368
Product: sc8180x-af					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SC81-240723/2369
Product: sc8180xp-aa					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SC81-240723/2370
Product: sc8180xp-aaab					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SC81-240723/2371
Product: sc8180xp-ab					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SC81-240723/2372
Product: sc8180xp-ac					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SC81-240723/2373
Product: sc8180xp-acaf					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while	https://www.qualcomm.com/company/product-	H-QUA-SC81-240723/2374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	security/bulletins/july-2023-bulletin	
Product: sc8180xp-ad					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SC81-240723/2375
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SC81-240723/2376
Product: sc8180xp-af					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SC81-240723/2377
Product: sc8180x\+sdx55					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SC81-240723/2378
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SC81-240723/2379
Product: sd460					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD46-240723/2380
Product: sd626					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD62-240723/2381
Integer Overflow	04-Jul-2023	7.8	Memory Corruption in Audio while	https://www.qualcomm	H-QUA-SD62-240723/2382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	.com/company/product-security/bulletins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD62-240723/2383
Product: sd660					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD66-240723/2384
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD66-240723/2385
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SD66-240723/2386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD66-240723/2387
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD66-240723/2388
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD66-240723/2389
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD66-240723/2390
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD66-240723/2391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD66-240723/2392
Product: sd662					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD66-240723/2393
Product: sd670					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD67-240723/2394
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD67-240723/2395
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD67-240723/2396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD67-240723/2397
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD67-240723/2398
Product: sd675					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD67-240723/2399
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD67-240723/2400
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/company/product-	H-QUA-SD67-240723/2401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD67-240723/2402
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD67-240723/2403
Product: sd730					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD73-240723/2404
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD73-240723/2405
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/compa	H-QUA-SD73-240723/2406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD73-240723/2407
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD73-240723/2408
Product: sd820					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD82-240723/2409
Product: sd821					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD82-240723/2410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sd835					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD83-240723/2411
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD83-240723/2412
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD83-240723/2413
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD83-240723/2414
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SD83-240723/2415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD83-240723/2416
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD83-240723/2417
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD83-240723/2418
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD83-240723/2419
Product: sd855					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SD85-240723/2420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command message received from network. **CVE ID : CVE-2023-21631**	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD85-240723/2421
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD85-240723/2422
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD85-240723/2423
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD85-240723/2424
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer	https://www.qualcomm.com/company/product-	H-QUA-SD85-240723/2425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD85-240723/2426
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD85-240723/2427
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD85-240723/2428
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD85-240723/2429
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD85-240723/2430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	etins/july-2023-bulletin	
Product: sd865_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD86-240723/2431
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD86-240723/2432
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD86-240723/2433
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD86-240723/2434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD86-240723/2435
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD86-240723/2436
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD86-240723/2437
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD86-240723/2438
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD86-240723/2439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD86-240723/2440
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD86-240723/2441
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD86-240723/2442
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD86-240723/2443
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD86-240723/2444
N/A	04-Jul-2023	5.5	Information disclosure in DSP	https://www.qualcomm	H-QUA-SD86-240723/2445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Services while loading dynamic module. **CVE ID : CVE-2023-21624**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: sd888					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD88-240723/2446
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD88-240723/2447
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD88-240723/2448
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SD88-240723/2449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD88-240723/2450
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD88-240723/2451
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD88-240723/2452
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD88-240723/2453
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD88-240723/2454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sdm429w					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SDM4-240723/2455
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SDM4-240723/2456
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SDM4-240723/2457
Product: sdx20m					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SDX2-240723/2458
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SDX2-240723/2459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	etins/july-2023-bulletin	
Product: sdx55					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SDX5-240723/2460
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SDX5-240723/2461
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SDX5-240723/2462
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SDX5-240723/2463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SDX5-240723/2464
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SDX5-240723/2465
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SDX5-240723/2466
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SDX5-240723/2467
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SDX5-240723/2468
Product: sdx57m					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SDX5-240723/2469
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SDX5-240723/2470
Product: sdx65m					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SDX6-240723/2471
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SDX6-240723/2472
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA	https://www.qualcomm.com/company/product-security/bull	H-QUA-SDX6-240723/2473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer release event about CFR data. **CVE ID : CVE-2023-28541**	etins/july-2023-bulletin	
Product: sd_455					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD_4-240723/2474
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD_4-240723/2475
Product: sd_675					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD_6-240723/2476
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD_6-240723/2477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	etins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD_6-240723/2478
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD_6-240723/2479
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD_6-240723/2480
Product: sd_8_gen1_5g					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD_8-240723/2481
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/compa	H-QUA-SD_8-240723/2482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	ny/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD_8-240723/2483
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD_8-240723/2484
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD_8-240723/2485
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SD_8-240723/2486
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD_8-240723/2487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	etins/july-2023-bulletin	
Product: sg4150p					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SG41-240723/2488
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SG41-240723/2489
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SG41-240723/2490
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SG41-240723/2491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SG41-240723/2492
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SG41-240723/2493
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SG41-240723/2494
Product: sm4125					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM41-240723/2495
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM41-240723/2496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM41-240723/2497
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM41-240723/2498
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM41-240723/2499
Product: sm6250					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM62-240723/2500
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SM62-240723/2501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM62-240723/2502
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM62-240723/2503
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM62-240723/2504
Product: sm6250p					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM62-240723/2505
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SM62-240723/2506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	etins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM62-240723/2507
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM62-240723/2508
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM62-240723/2509
Product: sm7250p					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM72-240723/2510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM72-240723/2511
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM72-240723/2512
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM72-240723/2513
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM72-240723/2514
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM72-240723/2515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM72-240723/2516
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM72-240723/2517
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM72-240723/2518
Product: sm7315					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM73-240723/2519
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/company/product-security/bull	H-QUA-SM73-240723/2520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM73-240723/2521
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM73-240723/2522
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM73-240723/2523
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM73-240723/2524
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SM73-240723/2525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM73-240723/2526
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM73-240723/2527
Product: sm7325p					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM73-240723/2528
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM73-240723/2529
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM	https://www.qualcomm	H-QUA-SM73-240723/2530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	.com/company/product-security/bulletins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM73-240723/2531
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM73-240723/2532
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM73-240723/2533
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM73-240723/2534
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while	https://www.qualcomm.com/company/product-	H-QUA-SM73-240723/2535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SM73-240723/2536
Product: smart_audio_200					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SMAR-240723/2537
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SMAR-240723/2538
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SMAR-240723/2539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SMAR-240723/2540
Product: smart_audio_400					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SMAR-240723/2541
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SMAR-240723/2542
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SMAR-240723/2543
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/company/product-security/bull	H-QUA-SMAR-240723/2544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SMAR-240723/2545
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SMAR-240723/2546
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SMAR-240723/2547
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SMAR-240723/2548
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SMAR-240723/2549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
Product: smart_display_200					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SMAR-240723/2550
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SMAR-240723/2551
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SMAR-240723/2552
Product: snapdragon_208					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2554
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2555
Product: snapdragon_210					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2556
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2557
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/company/product-security/bull	H-QUA-SNAP-240723/2558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	etins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2559
Product: snapdragon_212					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2560
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2561
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2563
Product: snapdragon_425					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2564
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2565
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2566
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while	https://www.qualcomm.com/company/product-security/bull	H-QUA-SNAP-240723/2567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	etins/july-2023-bulletin	
Product: snapdragon_427					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2568
Product: snapdragon_429					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2569
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2570
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2572
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2573
Product: snapdragon_430					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2574
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2575
Product: snapdragon_435					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2576
Product: snapdragon_439					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2577
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2578
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2579
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/company/product-security/bull	H-QUA-SNAP-240723/2580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2581
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2582
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2583
Product: snapdragon_450					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2584
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while	https://www.qualcomm.com/compa	H-QUA-SNAP-240723/2585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	ny/product-security/bulletins/july-2023-bulletin	
Product: snapdragon_460					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2586
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2587
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2588
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2590
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2591
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2592
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2593
Product: snapdragon_480\+_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command message received from network. **CVE ID : CVE-2023-21631**	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2595
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2596
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2597
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2598
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SNAP-240723/2599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24854	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2600
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2601
Product: snapdragon_480_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2602
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2604
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2605
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2606
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2607
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2608
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to	https://www.qualcomm	H-QUA-SNAP-240723/2609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: snapdragon_4_gen_1					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2610
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2611
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2612
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2614
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2615
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2616
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2617
Product: snapdragon_4_gen_2					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command message received from network. **CVE ID : CVE-2023-21631**	2023-bulletin	
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2619
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2620
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2621
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2622
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/company/product-	H-QUA-SNAP-240723/2623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2624
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2625
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2626
Product: snapdragon_625					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2627
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/compa	H-QUA-SNAP-240723/2628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	ny/product-security/bulletins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2629
Product: snapdragon_626					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2630
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2631
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2632
Product: snapdragon_630					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2633
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2634
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2635
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2636
Product: snapdragon_632					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/company/product-security/bull	H-QUA-SNAP-240723/2637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	etins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2638
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2639
Product: snapdragon_636					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2640
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2642
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2643
Product: snapdragon_660					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2644
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2645
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/company/product-security/bull	H-QUA-SNAP-240723/2646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	etins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2647
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2648
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2649
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2650
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2652
Product: snapdragon_662					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2653
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2654
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2655
Integer Overflow	04-Jul-2023	7.8	Memory Corruption in Audio while	https://www.qualcomm	H-QUA-SNAP-240723/2656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	.com/company/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2657
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2658
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2659
Product: snapdragon_665					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21631		
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2661
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2662
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2663
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2664
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_670					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2666
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2667
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2668
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2669
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: snapdragon_675					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2671
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2672
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2673
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2674
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SNAP-240723/2675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	etins/july-2023-bulletin	
Product: snapdragon_678					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2676
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2677
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2678
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2679
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while	https://www.qualcomm.com/company/product-	H-QUA-SNAP-240723/2680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	security/bulletins/july-2023-bulletin	
Product: snapdragon_680_4g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2681
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2682
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2683
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2685
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2686
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2687
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2688
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_685_4g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2690
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2691
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2692
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2693
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/compa	H-QUA-SNAP-240723/2694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2695
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2696
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2697
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2698
Product: snapdragon_690_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in	https://www.qualcomm.com/compa	H-QUA-SNAP-240723/2699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2700
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2701
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2702
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2704
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2705
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2706
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2707
Product: snapdragon_695_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received from network. **CVE ID : CVE-2023-21631**		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2709
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2710
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2711
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2712
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24854	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2714
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2715
Product: snapdragon_710					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2716
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2717
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SNAP-240723/2718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2719
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2720
Product: snapdragon_712					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2721
Product: snapdragon_720g					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2723
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2724
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2725
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2726
Product: snapdragon_730					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21633		
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2728
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2729
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2730
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2731
Product: snapdragon_730g					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsReg	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			isterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2733
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2734
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2735
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2736
Product: snapdragon_732g					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing	https://www.qualcomm.com/compa	H-QUA-SNAP-240723/2737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	ny/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2738
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2739
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2740
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2741
Product: snapdragon_750g_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper	https://www.qualcomm	H-QUA-SNAP-240723/2742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	.com/company/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2743
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2744
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2745
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2747
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2748
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2749
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2750
Product: snapdragon_765g_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received from network. **CVE ID : CVE-2023-21631**		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2752
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2753
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2754
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2755
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24851	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2757
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2758
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2759
Product: snapdragon_765_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2761
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2762
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2763
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2764
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2766
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2767
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2768
Product: snapdragon_768g_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2769
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsReg	https://www.qualcomm.com/company/product-security/bull	H-QUA-SNAP-240723/2770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			isterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2771
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2772
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2773
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2774
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24854	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2776
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2777
Product: snapdragon_778g\+					
Affected Version(s): -					
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2778
Product: snapdragon_778g\+_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2780
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2781
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2782
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2783
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2785
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2786
Product: snapdragon_778g_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2787
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2788
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/company/product-security/bull	H-QUA-SNAP-240723/2789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	etins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2790
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2791
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2792
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2793
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2795
Product: snapdragon_780g					
Affected Version(s): -					
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2796
Product: snapdragon_780g_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2797
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2799
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2800
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2801
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2802
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2803
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to	https://www.qualcomm	H-QUA-SNAP-240723/2804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: snapdragon_782g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2805
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2806
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2807
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2809
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2810
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2811
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2812
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_7c					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2814
Product: snapdragon_7c\+_gen_3					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2815
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2816
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2817
Integer Overflow	04-Jul-2023	7.8	Memory Corruption in Audio while	https://www.qualcomm	H-QUA-SNAP-240723/2818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	.com/company/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2819
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2820
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2821
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2822
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while	https://www.qualcomm.com/company/product-	H-QUA-SNAP-240723/2823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			loading dynamic module. **CVE ID : CVE-2023-21624**	security/bulletins/july-2023-bulletin	
Product: snapdragon_7c_gen_2					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2824
Product: snapdragon_820					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2825
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2826
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2828
Product: snapdragon_821					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2829
Product: snapdragon_835					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2830
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2831
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SNAP-240723/2832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24851	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2833
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2834
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2835
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2836
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: snapdragon_845					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2838
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2839
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2840
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2841
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
Product: snapdragon_850					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2843
Product: snapdragon_855					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2844
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2845
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21635	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2847
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2848
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2849
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2850
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2852
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2853
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2854
Product: snapdragon_855\+\/860					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2856
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2857
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2858
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2859
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2861
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2862
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2863
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2864
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2865
Product: snapdragon_865					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2866
Product: snapdragon_865\+					
Affected Version(s): -					
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2867
Product: snapdragon_865\+_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2868
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2870
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2871
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2872
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2873
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2875
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2876
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2877
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2878
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2879
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to	https://www.qualcomm	H-QUA-SNAP-240723/2880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: snapdragon_865_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2881
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2882
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2883
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21637	2023-bulletin	
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2885
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2886
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2887
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2888
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2890
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2891
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2892
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2893
Product: snapdragon_870					
Affected Version(s): -					
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_870_5					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2895
Product: snapdragon_870_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2896
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2897
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2899
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2900
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2901
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2902
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2904
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2905
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2906
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2907
Product: snapdragon_888					
Affected Version(s): -					
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_888\+					
Affected Version(s): -					
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2909
Product: snapdragon_888\+_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2910
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2911
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2912
Integer Overflow	04-Jul-2023	7.8	Memory Corruption in Audio while	https://www.qualcomm	H-QUA-SNAP-240723/2913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	.com/company/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2914
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2915
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2916
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2917
Product: snapdragon_888_5g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2918
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2919
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2920
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2921
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2923
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2924
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2925
Product: snapdragon_8\+_gen_1					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2926
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while	https://www.qualcomm	H-QUA-SNAP-240723/2927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	.com/company/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2928
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2929
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2930
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2931
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN	https://www.qualcomm.com/compa	H-QUA-SNAP-240723/2932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firmware response message. **CVE ID : CVE-2023-24854**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2933
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2934
Product: snapdragon_8_gen_1					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2935
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21638	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux when the file upload API is called with parameters having large buffer. **CVE ID : CVE-2023-21640**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2937
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2938
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2939
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2940
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2942
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2943
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2944
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2945
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2947
Product: snapdragon_ar2_gen_1					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2948
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2949
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2950
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24851	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2952
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2953
Product: snapdragon_auto_4g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2954
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2955
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM	https://www.qualcomm	H-QUA-SNAP-240723/2956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	.com/company/product-security/bulletins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2957
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2958
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2959
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2960
Product: snapdragon_auto_5g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2961
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2962
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2963
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2964
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2966
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2967
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2968
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2969
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_w5\+_gen_1					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2971
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2972
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2973
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2974
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer	https://www.qualcomm.com/company/product-	H-QUA-SNAP-240723/2975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	security/bulletins/july-2023-bulletin	
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2976
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2977
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2978
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2979
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN	https://www.qualcomm.com/company/product-	H-QUA-SNAP-240723/2980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firmware response message. **CVE ID : CVE-2023-24854**	security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2981
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2982
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2983
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2984
Product: snapdragon_wear_1300					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in	https://www.qualcomm.com/compa	H-QUA-SNAP-240723/2985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	ny/product-security/bulletins/july-2023-bulletin	
Product: snapdragon_wear_2100					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2986
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2987
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2988
Product: snapdragon_wear_2500					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2989
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2990
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2991
Product: snapdragon_wear_3100					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2993
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2994
Product: snapdragon_wear_4100\+					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2995
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2996
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/2997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2998
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/2999
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3000
Product: snapdragon_x12					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3001
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/3002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3003
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3004
Product: snapdragon_x12_lte					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3005
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3006
Product: snapdragon_x20					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3007
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3008
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3009
Product: snapdragon_x24					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3010
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/company/product-security/bull	H-QUA-SNAP-240723/3011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	etins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3012
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3013
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3014
Product: snapdragon_x5					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3015
Product: snapdragon_x50_5g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3016
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3017
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3018
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3019
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/3020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3021
Product: snapdragon_x55_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3022
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3023
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3025
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3026
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3027
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3028
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3030
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3031
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3032
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3033
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3034
N/A	04-Jul-2023	5.5	Information disclosure in DSP	https://www.qualcomm	H-QUA-SNAP-240723/3035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Services while loading dynamic module. **CVE ID : CVE-2023-21624**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: snapdragon_x65_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3036
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3037
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3038
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/3039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24851	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3040
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3041
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3042
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3043
Product: snapdragon_x70					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/3044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command message received from network. **CVE ID : CVE-2023-21631**	2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3045
Product: snapdragon_xr1					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3046
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3047
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3049
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3050
Product: snapdragon_xr2\+_gen_1					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3051
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3052
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3054
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3055
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3056
Product: snapdragon_xr2_5g					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3057
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsReg	https://www.qualcomm.com/company/product-security/bull	H-QUA-SNAP-240723/3058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			isterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3059
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3060
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3061
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3062
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/company/product-	H-QUA-SNAP-240723/3063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3064
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3065
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3066
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3067
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SNAP-240723/3068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3069
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3070
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SNAP-240723/3071
Product: ssg2115p					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SSG2-240723/3072
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/company/product-	H-QUA-SSG2-240723/3073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SSG2-240723/3074
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SSG2-240723/3075
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SSG2-240723/3076
Product: ssg2125p					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SSG2-240723/3077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SSG2-240723/3078
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SSG2-240723/3079
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SSG2-240723/3080
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SSG2-240723/3081
Product: sw5100					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received from network. **CVE ID : CVE-2023-21631**		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3083
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3084
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3085
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3086
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or	https://www.qualcomm.com/company/product-	H-QUA-SW51-240723/3087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3088
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3089
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3090
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3091
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SW51-240723/3092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3093
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3094
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3095
Product: sw5100p					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3097
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3098
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3099
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3100
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21672		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3102
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3103
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3104
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3105
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3107
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3108
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SW51-240723/3109
Product: sxr1120					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR1-240723/3110
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SXR1-240723/3111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR1-240723/3112
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR1-240723/3113
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR1-240723/3114
Product: sxr1230p					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR1-240723/3115
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/company/product-	H-QUA-SXR1-240723/3116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR1-240723/3117
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR1-240723/3118
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR1-240723/3119
Product: sxr2130					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR2-240723/3120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR2-240723/3121
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR2-240723/3122
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR2-240723/3123
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR2-240723/3124
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR2-240723/3125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR2-240723/3126
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR2-240723/3127
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR2-240723/3128
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR2-240723/3129
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR2-240723/3130
N/A	04-Jul-2023	5.5	Information disclosure in DSP	https://www.qualcomm	H-QUA-SXR2-240723/3131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Services while loading dynamic module. **CVE ID : CVE-2023-21624**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: sxr2230p					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR2-240723/3132
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR2-240723/3133
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR2-240723/3134
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR2-240723/3135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-SXR2-240723/3136
Product: video_collaboration_vc1					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3137
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3138
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3139
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-VIDE-240723/3140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3141
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3142
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3143
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3144
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: video_collaboration_vc3					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3146
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3147
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3148
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3149
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/company/product-	H-QUA-VIDE-240723/3150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3151
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3152
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3153
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3154
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-VIDE-240723/3155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
Product: video_collaboration_vc5					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3156
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3157
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3158
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VIDE-240723/3159
Product: vision_intelligence_100					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/compa	H-QUA-VISI-240723/3160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	ny/product-security/bulletins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VISI-240723/3161
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VISI-240723/3162
Product: vision_intelligence_200					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VISI-240723/3163
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VISI-240723/3164
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while	https://www.qualcomm.com/compa	H-QUA-VISI-240723/3165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	ny/product-security/bulletins/july-2023-bulletin	
Product: vision_intelligence_300					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VISI-240723/3166
Product: vision_intelligence_400					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VISI-240723/3167
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VISI-240723/3168
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VISI-240723/3169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VISI-240723/3170
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-VISI-240723/3171
Product: wcd9306					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3172
Product: wcd9326					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21631		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3174
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3175
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3176
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3177
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3179
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3180
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3181
Product: wcd9335					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3182
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsReg	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCD9-240723/3183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			isterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3184
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3185
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3186
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3187
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCD9-240723/3188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24851	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3189
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3190
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3191
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3192
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wcd9340					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3194
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3195
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3196
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3197
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCD9-240723/3198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3199
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3200
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3201
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3202
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCD9-240723/3203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21624	2023-bulletin	
Product: wcd9341					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3204
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3205
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3206
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3208
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3209
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3210
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3211
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3213
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3214
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3215
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3216
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3217
N/A	04-Jul-2023	5.5	Information disclosure in DSP	https://www.qualcomm	H-QUA-WCD9-240723/3218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Services while loading dynamic module. **CVE ID : CVE-2023-21624**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: wcd9360					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3219
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3220
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3221
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCD9-240723/3222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3223
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3224
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3225
Product: wcd9370					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3227
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3228
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3229
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3230
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3232
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3233
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3234
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3235
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3236
N/A	04-Jul-2023	5.5	Information disclosure in DSP	https://www.qualcomm	H-QUA-WCD9-240723/3237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Services while loading dynamic module. **CVE ID : CVE-2023-21624**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: wcd9371					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3238
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3239
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3240
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3242
Product: wcd9375					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3243
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3244
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3245
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/compa	H-QUA-WCD9-240723/3246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	ny/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3247
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3248
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3249
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3250
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCD9-240723/3251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3252
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3253
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3254
Product: wcd9380					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3256
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3257
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3258
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3259
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux when the file upload API is called with parameters having large buffer. **CVE ID : CVE-2023-21640**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3261
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3262
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3263
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3264
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3266
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3267
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3268
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3269
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3270
N/A	04-Jul-2023	5.5	Information disclosure in DSP	https://www.qualcomm	H-QUA-WCD9-240723/3271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Services while loading dynamic module. **CVE ID : CVE-2023-21624**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: wcd9385					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3272
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3273
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3274
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCD9-240723/3275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22386	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3276
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3277
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3278
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3279
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCD9-240723/3280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3281
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3282
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCD9-240723/3283
Product: wcn3610					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3285
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3286
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3287
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3288
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3290
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3291
Product: wcn3615					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3292
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3293
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-240723/3294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	etins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3295
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3296
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3297
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3298
Product: wcn3620					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in	https://www.qualcomm.com/compa	H-QUA-WCN3-240723/3299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	ny/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3300
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3301
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3302
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3303
Product: wcn3660					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3304
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3305
Product: wcn3660b					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3306
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3307
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity	https://www.qualcomm.com/compa	H-QUA-WCN3-240723/3308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3309
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3310
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3311
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3312
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-240723/3313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24854	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3314
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3315
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3316
Product: wcn3680					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3317
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-240723/3318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	etins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3319
Product: wcn3680b					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3320
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3321
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21635		
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3323
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3324
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3325
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3326
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3328
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3329
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3330
Product: wcn3910					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3331
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-240723/3332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3333
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3334
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3335
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3336
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCN3-240723/3337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3338
Product: wcn3950					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3339
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3340
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3342
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3343
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3344
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3345
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3347
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3348
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3349
Product: wcn3980					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3350
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsReg	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-240723/3351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			isterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3352
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3353
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3354
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3355
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/compa	H-QUA-WCN3-240723/3356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	ny/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3357
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3358
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3359
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3360
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-240723/3361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3362
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3363
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3364
Product: wcn3988					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3366
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3367
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3368
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3369
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21672		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3371
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3372
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3373
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3374
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3376
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3377
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3378
Product: wcn3990					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3379
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsReg	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-240723/3380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			isterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3381
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3382
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3383
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3384
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCN3-240723/3385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24851	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3386
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3387
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3388
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3389
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN3-240723/3390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wcn6740					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN6-240723/3391
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN6-240723/3392
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN6-240723/3393
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN6-240723/3394
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/compa	H-QUA-WCN6-240723/3395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN6-240723/3396
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN6-240723/3397
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN6-240723/3398
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WCN6-240723/3399
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module.	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN6-240723/3400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21624	etins/july-2023-bulletin	
Product: wsa8810					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3401
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3402
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3403
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3405
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3406
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3407
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3408
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WSA8-240723/3409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3410
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3411
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3412
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3413
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3415
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3416
Product: wsa8815					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3417
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3418
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets	https://www.qualcomm.com/company/product-	H-QUA-WSA8-240723/3419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			detected on telephony. **CVE ID : CVE-2023-21635**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3420
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3421
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3422
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3423
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/compa	H-QUA-WSA8-240723/3424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	ny/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3425
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3426
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3427
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3428
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bull	H-QUA-WSA8-240723/3429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3430
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3431
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3432
Product: wsa8830					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3434
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3435
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3436
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3437
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux when the file upload API is called with parameters having large buffer. **CVE ID : CVE-2023-21640**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3439
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3440
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3441
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3442
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3444
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3445
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3446
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3447
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3448
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to	https://www.qualcomm	H-QUA-WSA8-240723/3449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	.com/company/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3450
Product: wsa8832					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3451
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3452
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	https://www.qualcomm.com/company/product-security/bull	H-QUA-WSA8-240723/3453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22386	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3454
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3455
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3456
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3457
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WSA8-240723/3458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3459
Product: wsa8835					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3460
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3461
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3463
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3464
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3465
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux when the file upload API is called with parameters having large buffer. **CVE ID : CVE-2023-21640**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3466
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3468
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3469
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3470
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3471
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3473
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3474
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3475
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3476
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	H-QUA-WSA8-240723/3477
Vendor: Tenda					
Product: ac10					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jul-2023	9.8	Tenda AC10 v15.03.06.26 was discovered to contain a command injection vulnerability via the mac parameter in the function formWriteFacMac. **CVE ID : CVE-2023-37144**	N/A	H-TEN-AC10-240723/3478
Out-of-bounds Write	10-Jul-2023	9.8	Tenda AC1206 V15.03.06.23 and AC10 V15.03.06.47 were discovered to contain a stack overflow in the wpapsk_crypto parameter in the fromSetWirelessRepeat function. **CVE ID : CVE-2023-37710**	N/A	H-TEN-AC10-240723/3479
Out-of-bounds Write	10-Jul-2023	9.8	Tenda AC1206 V15.03.06.23 and AC10 V15.03.06.47 were discovered to contain a stack overflow in the deviceId parameter in the saveParentControlInfo function. **CVE ID : CVE-2023-37711**	N/A	H-TEN-AC10-240723/3480
Product: ac1206					
Affected Version(s): -					
Out-of-bounds Write	10-Jul-2023	9.8	Tenda AC1206 V15.03.06.23 and AC10 V15.03.06.47	N/A	H-TEN-AC12-240723/3481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			were discovered to contain a stack overflow in the wpapsk_crypto parameter in the fromSetWirelessRepeat function. **CVE ID : CVE-2023-37710**		
Out-of-bounds Write	10-Jul-2023	9.8	Tenda AC1206 V15.03.06.23 and AC10 V15.03.06.47 were discovered to contain a stack overflow in the deviceId parameter in the saveParentControlInfo function. **CVE ID : CVE-2023-37711**	N/A	H-TEN-AC12-240723/3482
Out-of-bounds Write	10-Jul-2023	9.8	Tenda AC1206 V15.03.06.23, F1202 V1.2.0.20(408), and FH1202 V1.2.0.20(408) were discovered to contain a stack overflow in the page parameter in the fromSetIpBind function. **CVE ID : CVE-2023-37712**	N/A	H-TEN-AC12-240723/3483
Product: f1202					
Affected Version(s): -					
Out-of-bounds Write	10-Jul-2023	9.8	Tenda AC1206 V15.03.06.23, F1202 V1.2.0.20(408), and FH1202 V1.2.0.20(408) were	N/A	H-TEN-F120-240723/3484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a stack overflow in the page parameter in the fromSetIpBind function. **CVE ID : CVE-2023-37712**		
Product: fh1202					
Affected Version(s): -					
Out-of-bounds Write	10-Jul-2023	9.8	Tenda AC1206 V15.03.06.23, F1202 V1.2.0.20(408), and FH1202 V1.2.0.20(408) were discovered to contain a stack overflow in the page parameter in the fromSetIpBind function. **CVE ID : CVE-2023-37712**	N/A	H-TEN-FH12-240723/3485
Product: fh1203					
Affected Version(s): -					
Out-of-bounds Write	10-Jul-2023	9.8	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the ssid parameter in the form_fast_setting_wifi_set function. **CVE ID : CVE-2023-37700**	N/A	H-TEN-FH12-240723/3486
Out-of-bounds Write	10-Jul-2023	9.8	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the deviceId parameter	N/A	H-TEN-FH12-240723/3487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the addWifiMacFilter function. **CVE ID : CVE-2023-37701**		
Out-of-bounds Write	10-Jul-2023	9.8	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the deviceId parameter in the formSetDeviceName function. **CVE ID : CVE-2023-37702**	N/A	H-TEN-FH12-240723/3488
Out-of-bounds Write	10-Jul-2023	9.8	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function. **CVE ID : CVE-2023-37703**	N/A	H-TEN-FH12-240723/3489
Out-of-bounds Write	10-Jul-2023	9.8	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function. **CVE ID : CVE-2023-37704**	N/A	H-TEN-FH12-240723/3490
Out-of-bounds Write	10-Jul-2023	9.8	Tenda FH1203 V2.0.1.6 was discovered to	N/A	H-TEN-FH12-240723/3491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a stack overflow via the page parameter in the fromAddressNat function. **CVE ID : CVE-2023-37705**		
Out-of-bounds Write	10-Jul-2023	9.8	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the entrys parameter in the fromAddressNat function. **CVE ID : CVE-2023-37706**	N/A	H-TEN-FH12-240723/3492
Out-of-bounds Write	10-Jul-2023	9.8	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the page parameter in the fromVirtualSer function. **CVE ID : CVE-2023-37707**	N/A	H-TEN-FH12-240723/3493
Vendor: totolink					
Product: a3300r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-2023	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain an unauthenticated remote code execution (RCE) vulnerability via the lang parameter in	N/A	H-TOT-A330-240723/3494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the setLanguageCfg function. **CVE ID : CVE-2023-37170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-2023	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the admuser parameter in the setPasswordCfg function. **CVE ID : CVE-2023-37171**	N/A	H-TOT-A330-240723/3495
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-2023	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the ip parameter in the setDiagnosisCfg function. **CVE ID : CVE-2023-37172**	N/A	H-TOT-A330-240723/3496
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-2023	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the command parameter in the setTracerouteCfg function.	N/A	H-TOT-A330-240723/3497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37173		
Product: lr350					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jul-2023	9.8	TOTOLINK LR350 V9.3.5u.6369_B20220309 was discovered to contain a command injection vulnerability via the hostname parameter in the setOpModeCfg function. **CVE ID : CVE-2023-37145**	N/A	H-TOT-LR35-240723/3498
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jul-2023	9.8	TOTOLINK LR350 V9.3.5u.6369_B20220309 was discovered to contain a command injection vulnerability via the FileName parameter in the UploadFirmwareFile function. **CVE ID : CVE-2023-37146**	N/A	H-TOT-LR35-240723/3499
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jul-2023	9.8	TOTOLINK LR350 V9.3.5u.6369_B20220309 was discovered to contain a command injection vulnerability via the ussd parameter in the setUssd function. **CVE ID : CVE-2023-37148**	N/A	H-TOT-LR35-240723/3500
Improper Neutralization of Special	07-Jul-2023	9.8	TOTOLINK LR350 V9.3.5u.6369_B20220309 was discovered to contain a	N/A	H-TOT-LR35-240723/3501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			command injection vulnerability via the FileName parameter in the setUploadSetting function. **CVE ID : CVE-2023-37149**		
Vendor: tyan					
Product: s5552\/s5552gm2nr					
Affected Version(s): -					
Files or Directories Accessible to External Parties	05-Jul-2023	4.2	A CWE-552 "Files or Directories Accessible to External Parties" in the web interface of the Tyan S5552 BMC version 3.00 allows an unauthenticated remote attacker to retrieve the private key of the TLS certificate in use by the BMC via forced browsing. This can then be abused to perform Man-in-the-Middle (MitM) attacks against victims that access the web interface through HTTPS. **CVE ID : CVE-2023-2538**	N/A	H-TYA-S555-240723/3502
Product: s5552\/s5552gm4nr					
Affected Version(s): -					
Files or Directories Accessible to External Parties	05-Jul-2023	4.2	A CWE-552 "Files or Directories Accessible to External Parties" in the web interface of	N/A	H-TYA-S555-240723/3503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Tyan S5552 BMC version 3.00 allows an unauthenticated remote attacker to retrieve the private key of the TLS certificate in use by the BMC via forced browsing. This can then be abused to perform Man-in-the-Middle (MitM) attacks against victims that access the web interface through HTTPS. **CVE ID : CVE-2023-2538**		
Product: s5552\/s5552wgm4nr					
Affected Version(s): -					
Files or Directories Accessible to External Parties	05-Jul-2023	4.2	A CWE-552 "Files or Directories Accessible to External Parties" in the web interface of the Tyan S5552 BMC version 3.00 allows an unauthenticated remote attacker to retrieve the private key of the TLS certificate in use by the BMC via forced browsing. This can then be abused to perform Man-in-the-Middle (MitM) attacks against victims that access the web interface through HTTPS.	N/A	H-TYA-S555-240723/3504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2538		
Product: s5552\/s5552wgm4nr-ex					
Affected Version(s): -					
Files or Directories Accessible to External Parties	05-Jul-2023	4.2	A CWE-552 "Files or Directories Accessible to External Parties" in the web interface of the Tyan S5552 BMC version 3.00 allows an unauthenticated remote attacker to retrieve the private key of the TLS certificate in use by the BMC via forced browsing. This can then be abused to perform Man-in-the-Middle (MitM) attacks against victims that access the web interface through HTTPS. **CVE ID : CVE-2023-2538**	N/A	H-TYA-S555-240723/3505
Vendor: ui					
Product: cloud_key_gen2					
Affected Version(s): -					
N/A	01-Jul-2023	9	UniFi OS 3.1 introduces a misconfiguration on consoles running UniFi Network that allows users on a local network to access MongoDB. Applicable Cloud Keys that are both (1) running UniFi OS	N/A	H-UI-CLOU-240723/3506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1 and (2) hosting the UniFi Network application. "Applicable Cloud Keys" include the following: Cloud Key Gen2 and Cloud Key Gen2 Plus. **CVE ID : CVE-2023-31997**		
Product: cloud_key_gen2_plus					
Affected Version(s): -					
N/A	01-Jul-2023	9	UniFi OS 3.1 introduces a misconfiguration on consoles running UniFi Network that allows users on a local network to access MongoDB. Applicable Cloud Keys that are both (1) running UniFi OS 3.1 and (2) hosting the UniFi Network application. "Applicable Cloud Keys" include the following: Cloud Key Gen2 and Cloud Key Gen2 Plus. **CVE ID : CVE-2023-31997**	N/A	H-UI-CLOU-240723/3507
Vendor: Vmware					
Product: sd-wan_edge					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Jul-2023	7.5	VMware SD-WAN (Edge) contains a bypass authentication vulnerability. An unauthenticated attacker can download the Diagnostic bundle of the application under VMware SD-WAN Management. **CVE ID : CVE-2023-20899**	https://www.vmware.com/security/advisories/VMSA-2023-0015.html	H-VMW-SD-W-240723/3508
Vendor: westerndigital					
Product: my_cloud					
Affected Version(s): -					
Authentication Bypass by Spoofing	01-Jul-2023	9.8	An authentication bypass issue via spoofing was discovered in the token-based authentication mechanism that could allow an attacker to carry out an impersonation attack. This issue affects My Cloud OS 5 devices: before 5.26.202. **CVE ID : CVE-2023-22814**	https://www.westerndigital.com/support/product-security/wdc-23006-my-cloud-firmware-version-5-26-202	H-WES-MY_C-240723/3509
Product: my_cloud_dl2100					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	01-Jul-2023	9.8	An authentication bypass issue via spoofing was discovered in the token-based authentication mechanism that could allow an attacker to carry out an impersonation attack. This issue affects My Cloud OS 5 devices: before 5.26.202. **CVE ID : CVE-2023-22814**	https://www.westerndigital.com/support/product-security/wdc-23006-my-cloud-firmware-version-5-26-202	H-WES-MY_C-240723/3510
Product: my_cloud_dl4100					
Affected Version(s): -					
Authentication Bypass by Spoofing	01-Jul-2023	9.8	An authentication bypass issue via spoofing was discovered in the token-based authentication mechanism that could allow an attacker to carry out an impersonation attack. This issue affects My Cloud OS 5 devices: before 5.26.202.	https://www.westerndigital.com/support/product-security/wdc-23006-my-cloud-firmware-version-5-26-202	H-WES-MY_C-240723/3511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22814		
Product: my_cloud_ex2100					
Affected Version(s): -					
Authentication Bypass by Spoofing	01-Jul-2023	9.8	An authentication bypass issue via spoofing was discovered in the token-based authentication mechanism that could allow an attacker to carry out an impersonation attack. This issue affects My Cloud OS 5 devices: before 5.26.202. **CVE ID : CVE-2023-22814**	https://www.westerndigital.com/support/product-security/wdc-23006-my-cloud-firmware-version-5-26-202	H-WES-MY_C-240723/3512
Product: my_cloud_ex2_ultra					
Affected Version(s): -					
Authentication Bypass by Spoofing	01-Jul-2023	9.8	An authentication bypass issue via spoofing was discovered in the token-based authentication mechanism that could allow an attacker to carry out an impersonation attack.	https://www.westerndigital.com/support/product-security/wdc-23006-my-cloud-firmware-version-5-26-202	H-WES-MY_C-240723/3513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects My Cloud OS 5 devices: before 5.26.202. **CVE ID : CVE-2023-22814**		
Product: my_cloud_ex4100					
Affected Version(s): -					
Authentication Bypass by Spoofing	01-Jul-2023	9.8	An authentication bypass issue via spoofing was discovered in the token-based authentication mechanism that could allow an attacker to carry out an impersonation attack. This issue affects My Cloud OS 5 devices: before 5.26.202. **CVE ID : CVE-2023-22814**	https://www.westerndigital.com/support/product-security/wdc-23006-my-cloud-firmware-version-5-26-202	H-WES-MY_C-240723/3514
Product: my_cloud_mirror_g2					
Affected Version(s): -					
Authentication Bypass by Spoofing	01-Jul-2023	9.8	An authentication bypass issue via spoofing was discovered in the token-based authentication mechanism that	https://www.westerndigital.com/support/product-security/wdc-23006-my-	H-WES-MY_C-240723/3515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an attacker to carry out an impersonation attack. This issue affects My Cloud OS 5 devices: before 5.26.202. **CVE ID : CVE-2023-22814**	cloud-firmware-version-5-26-202	
Product: my_cloud_pr2100					
Affected Version(s): -					
Authentication Bypass by Spoofing	01-Jul-2023	9.8	An authentication bypass issue via spoofing was discovered in the token-based authentication mechanism that could allow an attacker to carry out an impersonation attack. This issue affects My Cloud OS 5 devices: before 5.26.202. **CVE ID : CVE-2023-22814**	https://www.westerndigital.com/support/product-security/wdc-23006-my-cloud-firmware-version-5-26-202	H-WES-MY_C-240723/3516
Product: my_cloud_pr4100					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	01-Jul-2023	9.8	An authentication bypass issue via spoofing was discovered in the token-based authentication mechanism that could allow an attacker to carry out an impersonation attack. This issue affects My Cloud OS 5 devices: before 5.26.202. **CVE ID : CVE-2023-22814**	https://www.westerndigital.com/support/product-security/wdc-23006-my-cloud-firmware-version-5-26-202	H-WES-MY_C-240723/3517
Product: wd_cloud					
Affected Version(s): -					
Authentication Bypass by Spoofing	01-Jul-2023	9.8	An authentication bypass issue via spoofing was discovered in the token-based authentication mechanism that could allow an attacker to carry out an impersonation attack. This issue affects My Cloud OS 5 devices: before 5.26.202. **CVE ID : CVE-2023-22814**	https://www.westerndigital.com/support/product-security/wdc-23006-my-cloud-firmware-version-5-26-202	H-WES-WD_C-240723/3518
Operating System					
Vendor: ami					
Product: megarac_sp-x					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 12					
Use of Hard-coded Credentials	05-Jul-2023	9.8	AMI SPx contains a vulnerability in the BMC where an Attacker may cause a use of hard-coded cryptographic key by a hard-coded certificate. A successful exploit of this vulnerability may lead to a loss of confidentiality, integrity, and availability. **CVE ID : CVE-2023-34338**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023006.pdf	O-AMI-MEGA-250723/3519
Inadequate Encryption Strength	05-Jul-2023	8.8	AMI SPx contains a vulnerability in the BMC where a user may cause an inadequate encryption strength by hash-based message authentication code (HMAC). A successful exploit of this vulnerability may lead to a loss of confidentiality, integrity, and availability. **CVE ID : CVE-2023-34337**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023006.pdf	O-AMI-MEGA-250723/3520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	05-Jul-2023	8.8	AMI SPx contains a vulnerability in the BMC where a valid user may cause a use of hard-coded credentials. A successful exploit of this vulnerability may lead to a loss of confidentiality, integrity, and availability. **CVE ID : CVE-2023-34473**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023006.pdf	O-AMI-MEGA-250723/3521
N/A	05-Jul-2023	8.1	AMI SPx contains a vulnerability in the BMC where a user may cause a missing cryptographic step by generating a hash-based message authentication code (HMAC). A successful exploit of this vulnerability may lead to the loss confidentiality, integrity, and authentication. **CVE ID : CVE-2023-34471**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023006.pdf	O-AMI-MEGA-250723/3522
N/A	05-Jul-2023	6.5	AMI SPx contains a vulnerability in the BMC where an Attacker may cause an improper	https://9443417.fs1.hubspotusercontent-na1.net/hubf	O-AMI-MEGA-250723/3523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			neutralization of CRLF sequences in HTTP Headers. A successful exploit of this vulnerability may lead to a loss of integrity. **CVE ID : CVE-2023-34472**	s/9443417/Security%20Advisories/AMI-SA-2023006.pdf	
Affected Version(s): 13					
Use of Hard-coded Credentials	05-Jul-2023	9.8	AMI SPx contains a vulnerability in the BMC where an Attacker may cause a use of hard-coded cryptographic key by a hard-coded certificate. A successful exploit of this vulnerability may lead to a loss of confidentiality, integrity, and availability. **CVE ID : CVE-2023-34338**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023006.pdf	O-AMI-MEGA-250723/3524
Inadequate Encryption Strength	05-Jul-2023	8.8	AMI SPx contains a vulnerability in the BMC where a user may cause an inadequate encryption strength by hash-based message authentication code (HMAC). A successful	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023006.pdf	O-AMI-MEGA-250723/3525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit of this vulnerability may lead to a loss of confidentiality, integrity, and availability. **CVE ID : CVE-2023-34337**		
Use of Hard-coded Credentials	05-Jul-2023	8.8	AMI SPx contains a vulnerability in the BMC where a valid user may cause a use of hard-coded credentials. A successful exploit of this vulnerability may lead to a loss of confidentiality, integrity, and availability. **CVE ID : CVE-2023-34473**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023006.pdf	O-AMI-MEGA-250723/3526
N/A	05-Jul-2023	8.1	AMI SPx contains a vulnerability in the BMC where a user may cause a missing cryptographic step by generating a hash-based message authentication code (HMAC). A successful	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023006.pdf	O-AMI-MEGA-250723/3527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit of this vulnerability may lead to the loss confidentiality, integrity, and authentication. **CVE ID : CVE-2023-34471**		
N/A	05-Jul-2023	6.5	AMI SPx contains a vulnerability in the BMC where an Attacker may cause an improper neutralization of CRLF sequences in HTTP Headers. A successful exploit of this vulnerability may lead to a loss of integrity. **CVE ID : CVE-2023-34472**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023006.pdf	O-AMI-MEGA-250723/3528
Vendor: Arubanetworks					
Product: arubaos					
Affected Version(s): From (including) 10.4.0.0 Up to (excluding) 10.4.0.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jul-2023	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the underlying operating system. **CVE ID : CVE-2023-35975**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jul-2023	7.5	There is an unauthenticated buffer overflow vulnerability in the process controlling the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in a Denial-of-Service (DoS) condition affecting the web-based management interface of the controller. **CVE ID : CVE-2023-35979**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3530
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	An authenticated remote command injection vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system on the device running ArubaOS. **CVE ID : CVE-2023-35972**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35973**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3532
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35974**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3533
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access	https://www.arubanetworks.com/assets/alert/A	O-ARU-ARUB-250723/3534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35976**	RUBA-PSA-2023-008.txt	
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35977**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3535
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in the ArubaOS web-based management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35971**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in ArubaOS could allow an unauthenticated remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based management interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35978**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3537
Affected Version(s): From (including) 6.5.4.0 Up to (excluding) 8.6.0.21					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jul-2023	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35975		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jul-2023	7.5	There is an unauthenticated buffer overflow vulnerability in the process controlling the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in a Denial-of-Service (DoS) condition affecting the web-based management interface of the controller. **CVE ID : CVE-2023-35979**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3539
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	An authenticated remote command injection vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35972		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35973**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3541
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35974**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3542
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35976**		
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35977**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3544
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in the ArubaOS web-based management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35971**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in ArubaOS could allow an unauthenticated remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based management interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35978**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3546
Affected Version(s): From (including) 8.11.0.0 Up to (excluding) 8.11.1.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jul-2023	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-35975**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jul-2023	7.5	There is an unauthenticated buffer overflow vulnerability in the process controlling the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in a Denial-of-Service (DoS) condition affecting the web-based management interface of the controller. **CVE ID : CVE-2023-35979**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3548
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	An authenticated remote command injection vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-35972**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35973**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3550
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35974**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3551
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35976**		
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35977**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3553
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in the ArubaOS web-based management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the context of the affected interface. **CVE ID : CVE-2023-35971**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in ArubaOS could allow an unauthenticated remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based management interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35978**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3555
Affected Version(s): From (including) 8.7.0.0 Up to (excluding) 8.10.0.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jul-2023	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-35975**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jul-2023	7.5	There is an unauthenticated buffer overflow vulnerability in the process controlling the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in a Denial-of-Service (DoS) condition affecting the web-based management interface of the controller. **CVE ID : CVE-2023-35979**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3557
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	An authenticated remote command injection vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-35972**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35973**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3559
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Jul-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-35974**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3560
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35976**		
N/A	05-Jul-2023	6.5	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-35977**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3562
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in the ArubaOS web-based management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the context of the affected interface. **CVE ID : CVE-2023-35971**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jul-2023	6.1	A vulnerability in ArubaOS could allow an unauthenticated remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based management interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-35978**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-008.txt	O-ARU-ARUB-250723/3564
Vendor: Cisco					
Product: nx-os					
Affected Version(s): 14.0\\(1h\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.0\\(2c\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-	O-CIS-NX-O-250723/3566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**	cloudsec-enc-Vs5Wn2sX	
Affected Version(s): 14.0\\(3c\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.0\\(3d\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.1\\(1i\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.1\\(1j\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.1\\(1k\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.1\\(1l\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.1\\(2g\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.1\\(2m\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-NX-O-250723/3574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**	visory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	
Affected Version(s): 14.1\\(2o\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.1\\(2s\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.1\\(2u\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.1\\(2w\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.1\\(2x\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(1i\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(1j\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(1l\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-NX-O-250723/3582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**	visory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	
Affected Version(s): 14.2\\(2e\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(2f\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(2g\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(3j\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(3l\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(3n\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(3q\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(4i\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-NX-O-250723/3590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**	visory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	
Affected Version(s): 14.2\\(4k\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(4o\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(4p\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(5k\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(5l\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(5n\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(6d\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(6g\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-NX-O-250723/3598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**	visory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	
Affected Version(s): 14.2\\(6h\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(6l\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(6o\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(7f\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(7l\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(7q\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(7r\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(7s\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-NX-O-250723/3606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**	visory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	
Affected Version(s): 14.2\\(7t\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(7u\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(7v\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 14.2\\(7w\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.0\\(1k\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.0\\(1l\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.0\\(2e\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.0\\(2h\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-NX-O-250723/3614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**	visory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	
Affected Version(s): 15.1\\(1h\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.1\\(2e\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.1\\(3e\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.1\\(4c\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.2\\(1g\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.2\\(2e\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.2\\(2f\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.2\\(2g\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-NX-O-250723/3622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**	visory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	
Affected Version(s): 15.2\\(2h\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.2\\(3e\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.2\\(3f\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.2\\(3g\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.2\\(4d\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.2\\(4e\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.2\\(4f\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.2\\(5c\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-NX-O-250723/3630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**	visory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	
Affected Version(s): 15.2\\(5d\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.2\\(5e\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.2\\(6e\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.2\\(6g\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.2\\(7f\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.2\\(7g\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 15.2\\(8d\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 16.0\\(1g\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-NX-O-250723/3638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**	visory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	
Affected Version(s): 16.0\\(1j\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Affected Version(s): 16.0\\(2h\\)					
Inadequate Encryption Strength	12-Jul-2023	7.4	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX	O-CIS-NX-O-250723/3640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability. **CVE ID : CVE-2023-20185**		
Vendor: Citrix					
Product: hypervisor					
Affected Version(s): -					
N/A	04-Jul-2023	7.1	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where a guest OS may be able to control resources for which it is not authorized, which may lead to information disclosure and data tampering. **CVE ID : CVE-2023-25517**	https://nvidia.custhelp.com/app/answers/detail/a_id/5468	O-CIT-HYPE-250723/3641
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
Use After Free	05-Jul-2023	8.8	An attacker could have triggered a use-after-free condition when creating a	https://www.mozilla.org/security/advisories/mf	O-DEB-DEBI-250723/3642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WebRTC connection over HTTPS. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37201**	sa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	
Use After Free	05-Jul-2023	8.8	Cross-compartment wrappers wrapping a scripted proxy could have caused objects from other compartments to be stored in the main compartment resulting in a use-after-free. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37202**	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	O-DEB-DEBI-250723/3643
Out-of-bounds Write	05-Jul-2023	8.8	Memory safety bugs present in Firefox 114, Firefox ESR 102.12, and Thunderbird 102.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	O-DEB-DEBI-250723/3644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37211**		
N/A	05-Jul-2023	7.8	When opening Diagcab files, Firefox did not warn the user that these files may contain malicious code. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37208**	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	O-DEB-DEBI-250723/3645
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	05-Jul-2023	6.5	A website could have obscured the fullscreen notification by using a URL with a scheme handled by an external program, such as a mailto URL. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37207**	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	O-DEB-DEBI-250723/3646
Affected Version(s): 11.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	05-Jul-2023	8.8	An attacker could have triggered a use-after-free condition when creating a WebRTC connection over HTTPS. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37201**	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	O-DEB-DEBI-250723/3647
Use After Free	05-Jul-2023	8.8	Cross-compartment wrappers wrapping a scripted proxy could have caused objects from other compartments to be stored in the main compartment resulting in a use-after-free. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37202**	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	O-DEB-DEBI-250723/3648
Out-of-bounds Write	05-Jul-2023	8.8	Memory safety bugs present in Firefox 114, Firefox ESR 102.12, and Thunderbird 102.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://ww	O-DEB-DEBI-250723/3649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have been exploited to run arbitrary code. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37211**	w.mozilla.org/security/advisories/mfsa2023-24/	
N/A	05-Jul-2023	7.8	When opening Diagcab files, Firefox did not warn the user that these files may contain malicious code. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37208**	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	O-DEB-DEBI-250723/3650
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	05-Jul-2023	6.5	A website could have obscured the fullscreen notification by using a URL with a scheme handled by an external program, such as a mailto URL. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13.	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	O-DEB-DEBI-250723/3651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37207		
Affected Version(s): 12.0					
Use After Free	05-Jul-2023	8.8	An attacker could have triggered a use-after-free condition when creating a WebRTC connection over HTTPS. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37201**	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	O-DEB-DEBI-250723/3652
Use After Free	05-Jul-2023	8.8	Cross-compartment wrappers wrapping a scripted proxy could have caused objects from other compartments to be stored in the main compartment resulting in a use-after-free. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37202**	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	O-DEB-DEBI-250723/3653
Out-of-bounds Write	05-Jul-2023	8.8	Memory safety bugs present in Firefox 114, Firefox ESR 102.12, and Thunderbird 102.12. Some of these bugs showed evidence of	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.or	O-DEB-DEBI-250723/3654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37211**	g/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	
N/A	05-Jul-2023	7.8	When opening Diagcab files, Firefox did not warn the user that these files may contain malicious code. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37208**	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/advisories/mfsa2023-24/	O-DEB-DEBI-250723/3655
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	05-Jul-2023	6.5	A website could have obscured the fullscreen notification by using a URL with a scheme handled by an external program, such as a mailto URL. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 115,	https://www.mozilla.org/security/advisories/mfsa2023-23/, https://www.mozilla.org/security/advisories/mfsa2023-22/, https://www.mozilla.org/security/a	O-DEB-DEBI-250723/3656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox ESR < 102.13, and Thunderbird < 102.13. **CVE ID : CVE-2023-37207**	dvisories/mfsa2023-24/	
Vendor: Google					
Product: android					
Affected Version(s): 11.0					
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664741; Issue ID: ALPS07664741. **CVE ID : CVE-2023-20689**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3657
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664735; Issue ID: ALPS07664735.	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20690		
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664731; Issue ID: ALPS07664731. **CVE ID : CVE-2023-20691**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3659
Improper Handling of Exceptional Conditions	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664720; Issue ID: ALPS07664720. **CVE ID : CVE-2023-20692**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3660
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664711; Issue ID: ALPS07664711. **CVE ID : CVE-2023-20693**		
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3662
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028;	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3664
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3665
Access of Resource Using	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to	https://corp.mediatek.com/product-	O-GOO-ANDR-250723/3666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incompatible Type ('Type Confusion')			type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**	security-bulletin/July-2023	
Affected Version(s): 12.0					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3667
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07664735; Issue ID: ALPS07664735. **CVE ID : CVE-2023-20690**		
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664731; Issue ID: ALPS07664731. **CVE ID : CVE-2023-20691**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3669
Integer Overflow or Wraparound	04-Jul-2023	7.5	In wlan firmware, there is possible system crash due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664711; Issue ID: ALPS07664711. **CVE ID : CVE-2023-20693**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3671
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3672
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**		
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3674
Out-of-bounds Write	04-Jul-2023	6.7	In cmdq, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636133.	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20757		
Out-of-bounds Write	04-Jul-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629578; Issue ID: ALPS07629578. **CVE ID : CVE-2023-20760**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3676
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3677
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	O-GOO-ANDR-250723/3678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	bulletin/July-2023	
Out-of-bounds Write	04-Jul-2023	6.7	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585; Issue ID: ALPS07629584. **CVE ID : CVE-2023-20767**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3679
Access of Resource Using Incompatible Type ('Type Confusion')	04-Jul-2023	6.7	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800. **CVE ID : CVE-2023-20768**		
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3681
Out-of-bounds Read	04-Jul-2023	6.7	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07292228; Issue ID: ALPS07292228. **CVE ID : CVE-2023-20774**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3683
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Jul-2023	6.4	In display, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671046; Issue ID: ALPS07671046. **CVE ID : CVE-2023-20771**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3684
Out-of-bounds Read	04-Jul-2023	4.4	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07536951; Issue ID: ALPS07536951. **CVE ID : CVE-2023-20748**		
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130. **CVE ID : CVE-2023-20758**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3686
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601.	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20759		
Affected Version(s): 13.0					
Missing Authorization	04-Jul-2023	7.8	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07611449; Issue ID: ALPS07441735. **CVE ID : CVE-2023-20773**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3688
Out-of-bounds Write	04-Jul-2023	6.7	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667. **CVE ID : CVE-2023-20753**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3689
Out-of-bounds Write	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow.	https://corp.mediatek.com/product-security-	O-GOO-ANDR-250723/3690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07588343. **CVE ID : CVE-2023-20754**	bulletin/July-2023	
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064; Issue ID: ALPS07509605. **CVE ID : CVE-2023-20755**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3691
Integer Overflow or Wraparound	04-Jul-2023	6.7	In keyinstall, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07510064;	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07549928. **CVE ID : CVE-2023-20756**		
Out-of-bounds Write	04-Jul-2023	6.7	In cmdq, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636133. **CVE ID : CVE-2023-20757**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3693
Out-of-bounds Write	04-Jul-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629578; Issue ID: ALPS07629578. **CVE ID : CVE-2023-20760**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628582. **CVE ID : CVE-2023-20761**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3695
Out-of-bounds Write	04-Jul-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573237; Issue ID: ALPS07573202. **CVE ID : CVE-2023-20766**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3696
Out-of-bounds Write	04-Jul-2023	6.7	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585; Issue ID: ALPS07629584. **CVE ID : CVE-2023-20767**		
Missing Authorization	04-Jul-2023	6.7	In vow, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441796; Issue ID: ALPS07441796. **CVE ID : CVE-2023-20772**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3698
Out-of-bounds Read	04-Jul-2023	6.7	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07292228;	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07292228. **CVE ID : CVE-2023-20774**		
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3700
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jul-2023	5.5	Potential zip path traversal vulnerability in Calendar application prior to version 12.4.07.15 in Android 13 allows attackers to write arbitrary file. **CVE ID : CVE-2023-30678**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=07	O-GOO-ANDR-250723/3701
Out-of-bounds Read	04-Jul-2023	4.4	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07536951; Issue ID: ALPS07536951. **CVE ID : CVE-2023-20748**		
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130. **CVE ID : CVE-2023-20758**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3703
Out-of-bounds Write	04-Jul-2023	4.4	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601.	https://corp.mediatek.com/product-security-bulletin/July-2023	O-GOO-ANDR-250723/3704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20759		
Product: chrome_os					
Affected Version(s): -					
Out-of-bounds Read	03-Jul-2023	4.6	Out of bounds read in Google Security Processor firmware in Google Chrome on Chrome OS prior to 114.0.5735.90 allowed a local attacker to perform denial of service via physical access to the device. (Chromium security severity: Medium) **CVE ID : CVE-2023-3497**	https://chromereleases.googleblog.com/2023/05/stable-channel-update-for-desktop_30.html	O-GOO-CHRO-250723/3705
Vendor: heroelectronix					
Product: qubo_hcd01_firmware					
Affected Version(s): 1.38_20220125					
Missing Authentication for Critical Function	04-Jul-2023	8.8	Hero Qubo HCD01_02_V1.38_20220125 devices allow TELNET access with root privileges by default, without a password. **CVE ID : CVE-2023-22906**	N/A	O-HER-QUBO-250723/3706
Product: qubo_hcd02_firmware					
Affected Version(s): 1.38_20220125					
Missing Authentication for Critical Function	04-Jul-2023	8.8	Hero Qubo HCD01_02_V1.38_20220125 devices allow TELNET access with root privileges	N/A	O-HER-QUBO-250723/3707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by default, without a password. **CVE ID : CVE-2023-22906**		
Vendor: HP					
Product: hp-ux					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code via JNDI Injection. By sending a specially crafted request using the property clientRerouteServerListJNDIName, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249514. **CVE ID : CVE-2023-27867**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249514, https://www.ibm.com/support/pages/node/7010029	O-HP-HP-U-250723/3708
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked class instantiation when providing plugin	https://exchange.xforce.ibmcloud.com/vulnerabilities/249516, https://www.ibm.com/support/pages/node/7010029	O-HP-HP-U-250723/3709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			classes. By sending a specially crafted request using the named pluginClassName class, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249516. **CVE ID : CVE-2023-27868**		
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked logger injection. By sending a specially crafted request using the named traceFile property, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249517. **CVE ID : CVE-2023-27869**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249517, https://www.ibm.com/support/pages/node/7010029	O-HP-HP-U-250723/3710
Improper Restriction of Operations within the Bounds of	10-Jul-2023	7.8	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 db2set is vulnerable	https://www.ibm.com/support/pages/node/7010565, https://exch	O-HP-HP-U-250723/3711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			to a buffer overflow, caused by improper bounds checking. An attacker could overflow the buffer and execute arbitrary code. IBM X-Force ID: 252184. **CVE ID : CVE-2023-30431**	ange.xforce.ibmcloud.com/vulnerabilities/252184	
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 federated server is vulnerable to a denial of service as the server may crash when using a specially crafted wrapper using certain options. IBM X-Force ID: 253202. **CVE ID : CVE-2023-30442**	https://www.ibm.com/support/pages/node/7010561, https://exchange.xforce.ibmcloud.com/vulnerabilities/253202	O-HP-HP-U-250723/3712
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253357. **CVE ID : CVE-2023-30445**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253357, https://www.ibm.com/support/pages/node/7010557	O-HP-HP-U-250723/3713
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2	https://www.ibm.com/support/page	O-HP-HP-U-250723/3714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253361 . **CVE ID : CVE-2023-30446**	s/node/7010557, https://exchange.xforce.ibmcloud.com/vulnerabilities/253361	
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253436. **CVE ID : CVE-2023-30447**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253436, https://www.ibm.com/support/pages/node/7010557	O-HP-HP-U-250723/3715
N/A	10-Jul-2023	7.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253437.	https://exchange.xforce.ibmcloud.com/vulnerabilities/253437, https://www.ibm.com/support/pages/node/7010557	O-HP-HP-U-250723/3716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30448		
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query. IBM X-Force ID: 253439. **CVE ID : CVE-2023-30449**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253439, https://www.ibm.com/support/pages/node/7010557	O-HP-HP-U-250723/3717
Improper Privilege Management	10-Jul-2023	6.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to an information disclosure due to improper privilege management when certain federation features are used. IBM X-Force ID: 252046. **CVE ID : CVE-2023-29256**	https://www.ibm.com/support/pages/node/7010573, https://exchange.xforce.ibmcloud.com/vulnerabilities/252046	O-HP-HP-U-250723/3718
Vendor: Huawei					
Product: emui					
Affected Version(s): 11.0.1					
N/A	06-Jul-2023	7.5	Vulnerability of failures to capture exceptions in the communication framework. Successful exploitation of this	https://device.harmonyos.com/en/docs/security/update/security-bulletins-	O-HUA-EMUI-250723/3719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may cause features to perform abnormally. **CVE ID : CVE-2023-1691**	202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	
N/A	06-Jul-2023	7.5	Vulnerability of failures to capture exceptions in the communication framework. Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID : CVE-2023-1695**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-EMUI-250723/3720
Affected Version(s): 12.0.0					
Authorization Bypass Through User-Controlled Key	06-Jul-2023	9.8	Vulnerability of commands from the modem being intercepted in the atcmdserver module. Attackers may exploit this vulnerability to rewrite the non-volatile random-access memory (NVRAM), or facilitate the exploitation of other vulnerabilities. **CVE ID : CVE-2023-37242**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-EMUI-250723/3721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jul-2023	9.1	Buffer overflow vulnerability in the modem pinctrl module. Successful exploitation of this vulnerability may affect the integrity and availability of the modem. **CVE ID : CVE-2023-37245**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-EMUI-250723/3722
N/A	06-Jul-2023	7.5	Vulnerability of failures to capture exceptions in the communication framework. Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID : CVE-2023-1691**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-EMUI-250723/3723
N/A	06-Jul-2023	7.5	Vulnerability of failures to capture exceptions in the communication framework. Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID : CVE-2023-1695**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/sup	O-HUA-EMUI-250723/3724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				port/bulletin/2023/7/	
Exposure of Resource to Wrong Sphere	06-Jul-2023	5.3	Vulnerability of kernel raw address leakage in the hang detector module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-3456**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-EMUI-250723/3725
Affected Version(s): 12.0.1					
Out-of-bounds Read	06-Jul-2023	9.1	Vulnerability of missing input length verification in the distributed file system. Successful exploitation of this vulnerability may cause out-of-bounds read. **CVE ID : CVE-2023-37240**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-EMUI-250723/3726
N/A	06-Jul-2023	7.5	Vulnerability of failures to capture exceptions in the communication framework. Successful exploitation of this vulnerability may	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587	O-HUA-EMUI-250723/3727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause features to perform abnormally. **CVE ID : CVE-2023-1691**	168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	
N/A	06-Jul-2023	7.5	Vulnerability of failures to capture exceptions in the communication framework. Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID : CVE-2023-1695**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-EMUI-250723/3728
N/A	06-Jul-2023	7.5	Format string vulnerability in the distributed file system. Attackers who bypass the selinux permission can exploit this vulnerability to crash the program. **CVE ID : CVE-2023-37239**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-EMUI-250723/3729
Affected Version(s): 13.0.0					
Authorization Bypass Through User-	06-Jul-2023	9.8	Vulnerability of commands from the modem being intercepted in the atcmdserver module. Attackers may	https://device.harmonyos.com/en/docs/security/update/security-	O-HUA-EMUI-250723/3730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Key			exploit this vulnerability to rewrite the non-volatile random-access memory (NVRAM), or facilitate the exploitation of other vulnerabilities. **CVE ID : CVE-2023-37242**	bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	
Exposure of Resource to Wrong Sphere	05-Jul-2023	9.1	Key management vulnerability on system. Successful exploitation of this vulnerability may affect service availability and integrity. **CVE ID : CVE-2023-3455**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-EMUI-250723/3731
Out-of-bounds Read	06-Jul-2023	9.1	Vulnerability of missing input length verification in the distributed file system. Successful exploitation of this vulnerability may cause out-of-bounds read. **CVE ID : CVE-2023-37240**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-EMUI-250723/3732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jul-2023	9.1	Buffer overflow vulnerability in the modem pinctrl module. Successful exploitation of this vulnerability may affect the integrity and availability of the modem. **CVE ID : CVE-2023-37245**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-EMUI-250723/3733
N/A	06-Jul-2023	7.5	Vulnerability of failures to capture exceptions in the communication framework. Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID : CVE-2023-1691**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-EMUI-250723/3734
N/A	06-Jul-2023	7.5	Vulnerability of failures to capture exceptions in the communication framework. Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID : CVE-2023-1695**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/sup	O-HUA-EMUI-250723/3735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				port/bulletin/2023/7/	
NULL Pointer Dereference	06-Jul-2023	7.5	Vulnerability of incomplete input parameter verification in the communication framework module. Successful exploitation of this vulnerability may affect availability. **CVE ID : CVE-2023-34164**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-EMUI-250723/3736
N/A	06-Jul-2023	7.5	Format string vulnerability in the distributed file system. Attackers who bypass the selinux permission can exploit this vulnerability to crash the program. **CVE ID : CVE-2023-37239**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-EMUI-250723/3737
Improper Input Validation	06-Jul-2023	7.5	Input verification vulnerability in the WMS API. Successful exploitation of this vulnerability may cause the device to restart. **CVE ID : CVE-2023-37241**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://cons	O-HUA-EMUI-250723/3738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				umer.huawei.com/en/support/bulletin/2023/7/	
Exposure of Resource to Wrong Sphere	06-Jul-2023	5.3	Vulnerability of kernel raw address leakage in the hang detector module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-3456**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-EMUI-250723/3739
N/A	06-Jul-2023	5.3	Vulnerability of apps' permission to access a certain API being incompletely verified in the wireless projection module. Successful exploitation of this vulnerability may affect some wireless projection features. **CVE ID : CVE-2023-37238**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-EMUI-250723/3740
Product: harmonyos					
Affected Version(s): 2.0					
Authorization Bypass Through User-Controlled Key	06-Jul-2023	9.8	Vulnerability of commands from the modem being intercepted in the atcmdserver module. Attackers may	https://device.harmonyos.com/en/docs/security/update/security-	O-HUA-HARM-250723/3741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability to rewrite the non-volatile random-access memory (NVRAM), or facilitate the exploitation of other vulnerabilities. **CVE ID : CVE-2023-37242**	bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jul-2023	9.1	Buffer overflow vulnerability in the modem pinctrl module. Successful exploitation of this vulnerability may affect the integrity and availability of the modem. **CVE ID : CVE-2023-37245**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3742
Exposure of Resource to Wrong Sphere	06-Jul-2023	5.3	Vulnerability of kernel raw address leakage in the hang detector module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-3456**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3743
Affected Version(s): 2.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Jul-2023	7.5	Vulnerability of failures to capture exceptions in the communication framework. Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID : CVE-2023-1691**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3744
N/A	06-Jul-2023	7.5	Vulnerability of failures to capture exceptions in the communication framework. Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID : CVE-2023-1695**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3745
Affected Version(s): 2.0.1					
Out-of-bounds Read	06-Jul-2023	9.1	Vulnerability of missing input length verification in the distributed file system. Successful exploitation of this vulnerability may cause out-of-bounds read.	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei	O-HUA-HARM-250723/3746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37240	.com/en/support/bulletin/2023/7/	
N/A	06-Jul-2023	7.5	Vulnerability of failures to capture exceptions in the communication framework. Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID : CVE-2023-1691**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3747
N/A	06-Jul-2023	7.5	Vulnerability of failures to capture exceptions in the communication framework. Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID : CVE-2023-1695**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3748
N/A	06-Jul-2023	7.5	Format string vulnerability in the distributed file system. Attackers who bypass the selinux permission can exploit this vulnerability to crash the program.	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858,	O-HUA-HARM-250723/3749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37239	https://consumer.huawei.com/en/support/bulletin/2023/7/	
Exposure of Resource to Wrong Sphere	06-Jul-2023	5.3	Vulnerability of kernel raw address leakage in the hang detector module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-3456**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3750
Affected Version(s): 2.1					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jul-2023	9.1	Buffer overflow vulnerability in the modem pinctrl module. Successful exploitation of this vulnerability may affect the integrity and availability of the modem. **CVE ID : CVE-2023-37245**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3751
Exposure of Resource to Wrong Sphere	06-Jul-2023	5.3	Vulnerability of kernel raw address leakage in the hang detector module. Successful exploitation of this vulnerability may	https://device.harmonyos.com/en/docs/security/update/security-bulletins-	O-HUA-HARM-250723/3752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affect service confidentiality. **CVE ID : CVE-2023-3456**	202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	
Affected Version(s): 3.0.0					
Authorization Bypass Through User-Controlled Key	06-Jul-2023	9.8	Vulnerability of commands from the modem being intercepted in the atcmdserver module. Attackers may exploit this vulnerability to rewrite the non-volatile random-access memory (NVRAM), or facilitate the exploitation of other vulnerabilities. **CVE ID : CVE-2023-37242**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3753
Exposure of Resource to Wrong Sphere	05-Jul-2023	9.1	Key management vulnerability on system. Successful exploitation of this vulnerability may affect service availability and integrity. **CVE ID : CVE-2023-3455**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jul-2023	9.1	Vulnerability of missing input length verification in the distributed file system. Successful exploitation of this vulnerability may cause out-of-bounds read. **CVE ID : CVE-2023-37240**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3755
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jul-2023	9.1	Buffer overflow vulnerability in the modem pinctrl module. Successful exploitation of this vulnerability may affect the integrity and availability of the modem. **CVE ID : CVE-2023-37245**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3756
N/A	06-Jul-2023	7.5	Vulnerability of failures to capture exceptions in the communication framework. Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID : CVE-2023-1691**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/sup	O-HUA-HARM-250723/3757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				port/bulletin/2023/7/	
N/A	06-Jul-2023	7.5	Vulnerability of failures to capture exceptions in the communication framework. Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID : CVE-2023-1695**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3758
NULL Pointer Dereference	06-Jul-2023	7.5	Vulnerability of incomplete input parameter verification in the communication framework module. Successful exploitation of this vulnerability may affect availability. **CVE ID : CVE-2023-34164**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3759
N/A	06-Jul-2023	7.5	Format string vulnerability in the distributed file system. Attackers who bypass the selinux permission can exploit this vulnerability to crash the program.	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://cons	O-HUA-HARM-250723/3760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37239	umer.huawei.com/en/support/bulletin/2023/7/	
Improper Input Validation	06-Jul-2023	7.5	Input verification vulnerability in the WMS API. Successful exploitation of this vulnerability may cause the device to restart. **CVE ID : CVE-2023-37241**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3761
Exposure of Resource to Wrong Sphere	06-Jul-2023	5.3	Vulnerability of kernel raw address leakage in the hang detector module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-3456**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3762
N/A	06-Jul-2023	5.3	Vulnerability of apps' permission to access a certain API being incompletely verified in the wireless projection module. Successful exploitation of this vulnerability may	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587	O-HUA-HARM-250723/3763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affect some wireless projection features. **CVE ID : CVE-2023-37238**	168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	
Affected Version(s): 3.1.0					
Exposure of Resource to Wrong Sphere	05-Jul-2023	9.1	Key management vulnerability on system. Successful exploitation of this vulnerability may affect service availability and integrity. **CVE ID : CVE-2023-3455**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3764
Out-of-bounds Read	06-Jul-2023	9.1	Vulnerability of missing input length verification in the distributed file system. Successful exploitation of this vulnerability may cause out-of-bounds read. **CVE ID : CVE-2023-37240**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3765
N/A	06-Jul-2023	7.5	Vulnerability of failures to capture exceptions in the communication framework.	https://device.harmonyos.com/en/docs/security/update/secu	O-HUA-HARM-250723/3766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID : CVE-2023-1691**	rity-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	
N/A	06-Jul-2023	7.5	Vulnerability of failures to capture exceptions in the communication framework. Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID : CVE-2023-1695**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3767
NULL Pointer Dereference	06-Jul-2023	7.5	Vulnerability of incomplete input parameter verification in the communication framework module. Successful exploitation of this vulnerability may affect availability. **CVE ID : CVE-2023-34164**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3768
N/A	06-Jul-2023	7.5	Format string vulnerability in the distributed file	https://device.harmonyos.com/en/do	O-HUA-HARM-250723/3769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system. Attackers who bypass the selinux permission can exploit this vulnerability to crash the program. **CVE ID : CVE-2023-37239**	cs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	
Improper Input Validation	06-Jul-2023	7.5	Input verification vulnerability in the WMS API. Successful exploitation of this vulnerability may cause the device to restart. **CVE ID : CVE-2023-37241**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3770
Exposure of Resource to Wrong Sphere	06-Jul-2023	5.3	Vulnerability of kernel raw address leakage in the hang detector module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-3456**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Jul-2023	5.3	Vulnerability of apps' permission to access a certain API being incompletely verified in the wireless projection module. Successful exploitation of this vulnerability may affect some wireless projection features. **CVE ID : CVE-2023-37238**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202307-0000001587168858, https://consumer.huawei.com/en/support/bulletin/2023/7/	O-HUA-HARM-250723/3772
Vendor: IBM					
Product: aix					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code via JNDI Injection. By sending a specially crafted request using the property clientRerouteServerListJNDIName, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249514. **CVE ID : CVE-2023-27867**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249514, https://www.ibm.com/support/pages/node/7010029	O-IBM-AIX-250723/3773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked class instantiation when providing plugin classes. By sending a specially crafted request using the named pluginClassName class, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249516. **CVE ID : CVE-2023-27868**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249516, https://www.ibm.com/support/pages/node/7010029	O-IBM-AIX-250723/3774
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked logger injection. By sending a specially crafted request using the named traceFile property, an attacker could exploit this vulnerability to	https://exchange.xforce.ibmcloud.com/vulnerabilities/249517, https://www.ibm.com/support/pages/node/7010029	O-IBM-AIX-250723/3775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code on the system. IBM X-Force ID: 249517. **CVE ID : CVE-2023-27869**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Jul-2023	7.8	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 db2set is vulnerable to a buffer overflow, caused by improper bounds checking. An attacker could overflow the buffer and execute arbitrary code. IBM X-Force ID: 252184. **CVE ID : CVE-2023-30431**	https://www.ibm.com/support/pages/node/7010565, https://exchange.xforce.ibmcloud.com/vulnerabilities/252184	O-IBM-AIX-250723/3776
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 federated server is vulnerable to a denial of service as the server may crash when using a specially crafted wrapper using certain options. IBM X-Force ID: 253202. **CVE ID : CVE-2023-30442**	https://www.ibm.com/support/pages/node/7010561, https://exchange.xforce.ibmcloud.com/vulnerabilities/253202	O-IBM-AIX-250723/3777
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server)	https://exchange.xforce.ibmcloud.com/vulnerabilities/25335	O-IBM-AIX-250723/3778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253357. **CVE ID : CVE-2023-30445**	7, https://www.ibm.com/support/pages/node/7010557	
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253361 . **CVE ID : CVE-2023-30446**	https://www.ibm.com/support/pages/node/7010557, https://exchange.xforce.ibmcloud.com/vulnerabilities/253361	O-IBM-AIX-250723/3779
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253436. **CVE ID : CVE-2023-30447**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253436, https://www.ibm.com/support/pages/node/7010557	O-IBM-AIX-250723/3780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Jul-2023	7.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253437. **CVE ID : CVE-2023-30448**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253437, https://www.ibm.com/support/pages/node/7010557	O-IBM-AIX-250723/3781
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query. IBM X-Force ID: 253439. **CVE ID : CVE-2023-30449**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253439, https://www.ibm.com/support/pages/node/7010557	O-IBM-AIX-250723/3782
Improper Privilege Management	10-Jul-2023	6.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to an information disclosure due to improper privilege management when certain federation features are used. IBM X-Force ID: 252046.	https://www.ibm.com/support/pages/node/7010573, https://exchange.xforce.ibmcloud.com/vulnerabilities/252046	O-IBM-AIX-250723/3783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29256		
N/A	10-Jul-2023	4.3	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is vulnerable to insufficient audit logging. IBM X-Force ID: 245918. **CVE ID : CVE-2023-23487**	https://exchange.xforce.ibmcloud.com/vulnerabilities/245918, https://www.ibm.com/support/pages/node/7010567	O-IBM-AIX-250723/3784
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Jul-2023	9.1	A backup file vulnerability found in UniFi applications (Version 7.3.83 and earlier) running on Linux operating systems allows application administrators to execute malicious commands on the host device being restored. **CVE ID : CVE-2023-28365**	https://community.ui.com/releases/Security-Advisory-Bulletin-031-031/8c85fc64-e9a8-4082-9ec4-56b14effd545	O-LIN-LINU-250723/3785
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code via JNDI Injection. By sending a specially	https://exchange.xforce.ibmcloud.com/vulnerabilities/249514, https://www.ibm.com/support/page	O-LIN-LINU-250723/3786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted request using the property clientRerouteServer ListJNDIName, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249514. **CVE ID : CVE-2023-27867**	s/node/7010029	
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked class instantiation when providing plugin classes. By sending a specially crafted request using the named pluginClassName class, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249516. **CVE ID : CVE-2023-27868**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249516, https://www.ibm.com/support/pages/node/7010029	O-LIN-LINU-250723/3787
Improper Control of Generation of Code	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5	https://exchange.xforce.ibmcloud.com/vulnerabi	O-LIN-LINU-250723/3788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked logger injection. By sending a specially crafted request using the named traceFile property, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249517. **CVE ID : CVE-2023-27869**	lities/249517, https://www.ibm.com/support/pages/node/7010029	
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Jul-2023	7.8	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 db2set is vulnerable to a buffer overflow, caused by improper bounds checking. An attacker could overflow the buffer and execute arbitrary code. IBM X-Force ID: 252184. **CVE ID : CVE-2023-30431**	https://www.ibm.com/support/pages/node/7010565, https://exchange.xforce.ibmcloud.com/vulnerabilities/252184	O-LIN-LINU-250723/3789
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 federated server is vulnerable to a denial of service as the server may	https://www.ibm.com/support/pages/node/7010561, https://exchange.xforce.ibmcloud.co	O-LIN-LINU-250723/3790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash when using a specially crafted wrapper using certain options. IBM X-Force ID: 253202. **CVE ID : CVE-2023-30442**	m/vulnerabilities/253202	
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253357. **CVE ID : CVE-2023-30445**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253357, https://www.ibm.com/support/pages/node/7010557	O-LIN-LINU-250723/3791
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253361 . **CVE ID : CVE-2023-30446**	https://www.ibm.com/support/pages/node/7010557, https://exchange.xforce.ibmcloud.com/vulnerabilities/253361	O-LIN-LINU-250723/3792
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows	https://exchange.xforce.i	O-LIN-LINU-250723/3793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253436. **CVE ID : CVE-2023-30447**	bmcloud.com/vulnerabilities/253436, https://www.ibm.com/support/pages/node/7010557	
N/A	10-Jul-2023	7.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253437. **CVE ID : CVE-2023-30448**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253437, https://www.ibm.com/support/pages/node/7010557	O-LIN-LINU-250723/3794
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query. IBM X-Force ID: 253439. **CVE ID : CVE-2023-30449**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253439, https://www.ibm.com/support/pages/node/7010557	O-LIN-LINU-250723/3795
Improper Privilege	10-Jul-2023	6.5	IBM Db2 for Linux, UNIX and Windows (includes Db2	https://www.ibm.com/support/page	O-LIN-LINU-250723/3796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			Connect Server) 10.5, 11.1, and 11.5 is vulnerable to an information disclosure due to improper privilege management when certain federation features are used. IBM X-Force ID: 252046. **CVE ID : CVE-2023-29256**	s/node/7010573, https://exchange.xforce.ibmcloud.com/vulnerabilities/252046	
N/A	10-Jul-2023	4.3	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is vulnerable to insufficient audit logging. IBM X-Force ID: 245918. **CVE ID : CVE-2023-23487**	https://exchange.xforce.ibmcloud.com/vulnerabilities/245918, https://www.ibm.com/support/pages/node/7010567	O-LIN-LINU-250723/3797
NULL Pointer Dereference	04-Jul-2023	3.3	NVIDIA CUDA toolkit for Linux and Windows contains a vulnerability in the nvdisasm binary file, where an attacker may cause a NULL pointer dereference by providing a user with a malformed ELF file. A successful exploit of this vulnerability may	https://nvidia.custhelp.com/app/answers/detail/a_id/5469	O-LIN-LINU-250723/3798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to a partial denial of service. **CVE ID : CVE-2023-25523**		
Affected Version(s): * Up to (including) 6.4.2					
Use After Free	06-Jul-2023	5.5	An issue was discovered in the Linux kernel through 6.4.2. A crafted UDF filesystem image causes a use-after-free write operation in the udf_put_super and udf_close_lvid functions in fs/udf/super.c. **CVE ID : CVE-2023-37454**	https://lore.kernel.org/all/00000000000056e02f05dfb6e11a@google.com/T/	O-LIN-LINU-250723/3799
Out-of-bounds Read	06-Jul-2023	4.6	An issue was discovered in the USB subsystem in the Linux kernel through 6.4.2. There is an out-of-bounds and crash in read_descriptors in drivers/usb/core/sysfs.c. **CVE ID : CVE-2023-37453**	https://lore.kernel.org/all/00000000000c0ffe505fe86c9ca@google.com/T/, https://lore.kernel.org/all/00000000000e56434059580f86e@google.com/T/	O-LIN-LINU-250723/3800
Affected Version(s): 3.13					
Out-of-bounds Write	05-Jul-2023	7.8	Linux Kernel nftables Out-Of-Bounds Read/Write	https://lore.kernel.org/netfilter-	O-LIN-LINU-250723/3801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability; nft_byteorder poorly handled vm register contents when CAP_NET_ADMIN is in any user or network namespace **CVE ID : CVE-2023-35001**	devel/20230705121515.747251-1-cascardo@canonical.com/T/	
Affected Version(s): 5.9.0					
Use After Free	05-Jul-2023	7.8	Linux Kernel nftables Use-After-Free Local Privilege Escalation Vulnerability; `nft_chain_lookup_byid()` failed to check whether a chain was active and CAP_NET_ADMIN is in any user or network namespace **CVE ID : CVE-2023-31248**	https://lore.kernel.org/netfilter-devel/20230705121627.GC19489@breakpoint.cc/T/	O-LIN-LINU-250723/3802
Vendor: loxone					
Product: miniserver_go_gen_2_firmware					
Affected Version(s): * Up to (excluding) 14.1.5.9					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Jul-2023	7.2	The websocket configuration endpoint of the Loxone Miniserver Go Gen.2 before 14.1.5.9 allows remote authenticated administrators to inject arbitrary OS commands via the timezone parameter. **CVE ID : CVE-2023-36622**	N/A	O-LOX-MINI-250723/3803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 14.2					
Use of Hard-coded Credentials	05-Jul-2023	7.8	The root password of the Loxone Miniserver Go Gen.2 before 14.2 is calculated using hard-coded secrets and the MAC address. This allows a local user to calculate the root password and escalate privileges. **CVE ID : CVE-2023-36623**	N/A	O-LOX-MINI-250723/3804
Affected Version(s): * Up to (including) 14.0.3.28					
Missing Authorization	05-Jul-2023	7.8	Loxone Miniserver Go Gen.2 through 14.0.3.28 allows an authenticated operating system user to escalate privileges via the Sudo configuration. This allows the elevated execution of binaries without a password requirement. **CVE ID : CVE-2023-36624**	N/A	O-LOX-MINI-250723/3805
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute	https://exchange.xforce.ibmcloud.com/vulnerabilities/249514, https://ww	O-MIC-WIND-250723/3806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code via JNDI Injection. By sending a specially crafted request using the property clientRerouteServer ListJNDIName, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249514. **CVE ID : CVE-2023-27867**	w.ibm.com/support/pages/node/7010029	
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked class instantiation when providing plugin classes. By sending a specially crafted request using the named pluginClassName class, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249516. **CVE ID : CVE-2023-27868**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249516, https://www.ibm.com/support/pages/node/7010029	O-MIC-WIND-250723/3807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked logger injection. By sending a specially crafted request using the named traceFile property, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249517. **CVE ID : CVE-2023-27869**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249517, https://www.ibm.com/support/pages/node/7010029	O-MIC-WIND-250723/3808
Improper Privilege Management	10-Jul-2023	7.8	IBM Db2 on Windows 10.5, 11.1, and 11.5 may be vulnerable to a privilege escalation caused by at least one installed service using an unquoted service path. A local attacker could exploit this vulnerability to gain elevated privileges by inserting an executable file in the path of the affected service. IBM X-Force ID: 249194. **CVE ID : CVE-2023-27558**	https://www.ibm.com/support/pages/node/7010571, https://exchange.xforce.ibmcloud.com/vulnerabilities/249194	O-MIC-WIND-250723/3809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Jul-2023	7.8	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 db2set is vulnerable to a buffer overflow, caused by improper bounds checking. An attacker could overflow the buffer and execute arbitrary code. IBM X-Force ID: 252184. **CVE ID : CVE-2023-30431**	https://www.ibm.com/support/pages/node/7010565, https://exchange.xforce.ibmcloud.com/vulnerabilities/252184	O-MIC-WIND-250723/3810
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 federated server is vulnerable to a denial of service as the server may crash when using a specially crafted wrapper using certain options. IBM X-Force ID: 253202. **CVE ID : CVE-2023-30442**	https://www.ibm.com/support/pages/node/7010561, https://exchange.xforce.ibmcloud.com/vulnerabilities/253202	O-MIC-WIND-250723/3811
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain	https://exchange.xforce.ibmcloud.com/vulnerabilities/253357, https://www.ibm.com/support/pages/node/7010557	O-MIC-WIND-250723/3812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tables. IBM X-Force ID: 253357. **CVE ID : CVE-2023-30445**		
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253361 . **CVE ID : CVE-2023-30446**	https://www.ibm.com/support/pages/node/7010557, https://exchange.xforce.ibmcloud.com/vulnerabilities/253361	O-MIC-WIND-250723/3813
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253436. **CVE ID : CVE-2023-30447**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253436, https://www.ibm.com/support/pages/node/7010557	O-MIC-WIND-250723/3814
N/A	10-Jul-2023	7.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5	https://exchange.xforce.ibmcloud.com/vulnerabilities/253437, https://ww	O-MIC-WIND-250723/3815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253437. **CVE ID : CVE-2023-30448**	w.ibm.com/support/pages/node/7010557	
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query. IBM X-Force ID: 253439. **CVE ID : CVE-2023-30449**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253439, https://www.ibm.com/support/pages/node/7010557	O-MIC-WIND-250723/3816
Improper Privilege Management	10-Jul-2023	6.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to an information disclosure due to improper privilege management when certain federation features are used. IBM X-Force ID: 252046. **CVE ID : CVE-2023-29256**	https://www.ibm.com/support/pages/node/7010573, https://exchange.xforce.ibmcloud.com/vulnerabilities/252046	O-MIC-WIND-250723/3817
N/A	10-Jul-2023	4.3	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is	https://exchange.xforce.ibmcloud.com/vulnerabilities/24591	O-MIC-WIND-250723/3818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to insufficient audit logging. IBM X-Force ID: 245918. **CVE ID : CVE-2023-23487**	8, https://www.ibm.com/support/pages/node/7010567	
NULL Pointer Dereference	04-Jul-2023	3.3	NVIDIA CUDA toolkit for Linux and Windows contains a vulnerability in the nvdisasm binary file, where an attacker may cause a NULL pointer dereference by providing a user with a malformed ELF file. A successful exploit of this vulnerability may lead to a partial denial of service. **CVE ID : CVE-2023-25523**	https://nvidia.custhelp.com/app/answers/detail/a_id/5469	O-MIC-WIND-250723/3819
Product: windows_10_1507					
Affected Version(s): *					
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32040	O-MIC-WIND-250723/3820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32040		
Affected Version(s): * Up to (excluding) 10.0.10240.20048					
N/A	11-Jul-2023	9.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33154	O-MIC-WIND-250723/3821
N/A	11-Jul-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-32057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32057	O-MIC-WIND-250723/3822
N/A	11-Jul-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-32038**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32038	O-MIC-WIND-250723/3823
N/A	11-Jul-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35302**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35302	O-MIC-WIND-250723/3824
N/A	11-Jul-2023	8.8	USB Audio Class System Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35303**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35303	O-MIC-WIND-250723/3825
N/A	11-Jul-2023	8.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/3826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35300	ability/CVE-2023-35300	
N/A	11-Jul-2023	7.8	Windows MSHTML Platform Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32046**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046	O-MIC-WIND-250723/3827
N/A	11-Jul-2023	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21756**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21756	O-MIC-WIND-250723/3828
N/A	11-Jul-2023	7.8	Windows Online Certificate Status Protocol (OCSP) SnapIn Remote Code Execution Vulnerability **CVE ID : CVE-2023-35313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35313	O-MIC-WIND-250723/3829
N/A	11-Jul-2023	7.8	Microsoft VOLSNAP.SYS Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35312	O-MIC-WIND-250723/3830
N/A	11-Jul-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35299**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35299	O-MIC-WIND-250723/3831
N/A	11-Jul-2023	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/3832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35340	ability/CVE-2023-35340	
N/A	11-Jul-2023	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32053	O-MIC-WIND-250723/3833
N/A	11-Jul-2023	7.8	Windows Transaction Manager Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35328**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35328	O-MIC-WIND-250723/3834
N/A	11-Jul-2023	7.8	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35342**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35342	O-MIC-WIND-250723/3835
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32034	O-MIC-WIND-250723/3836
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32035**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32035	O-MIC-WIND-250723/3837
N/A	11-Jul-2023	7.5	OLE Automation Information Disclosure Vulnerability **CVE ID : CVE-2023-32042**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32042	O-MIC-WIND-250723/3838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	7.5	Windows CryptoAPI Denial of Service Vulnerability **CVE ID : CVE-2023-35339**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35339	O-MIC-WIND-250723/3839
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32044**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32044	O-MIC-WIND-250723/3840
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32045**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32045	O-MIC-WIND-250723/3841
N/A	11-Jul-2023	7.5	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-35297**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35297	O-MIC-WIND-250723/3842
N/A	11-Jul-2023	7.5	Windows Print Spooler Information Disclosure Vulnerability **CVE ID : CVE-2023-35325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35325	O-MIC-WIND-250723/3843
Concurrent Execution using Shared Resource with Improper Synchronization	11-Jul-2023	7.5	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35309**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35309	O-MIC-WIND-250723/3844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
N/A	11-Jul-2023	7.5	Windows Extended Negotiation Denial of Service Vulnerability **CVE ID : CVE-2023-35330**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35330	O-MIC-WIND-250723/3845
N/A	11-Jul-2023	7.5	Windows Peer Name Resolution Protocol Denial of Service Vulnerability **CVE ID : CVE-2023-35338**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35338	O-MIC-WIND-250723/3846
N/A	11-Jul-2023	7.4	Windows Netlogon Information Disclosure Vulnerability **CVE ID : CVE-2023-21526**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21526	O-MIC-WIND-250723/3847
N/A	11-Jul-2023	7.3	Volume Shadow Copy Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32054	O-MIC-WIND-250723/3848
N/A	11-Jul-2023	6.8	Windows Remote Desktop Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32043	O-MIC-WIND-250723/3849
N/A	11-Jul-2023	6.8	Windows Remote Desktop Protocol Security Feature Bypass **CVE ID : CVE-2023-35332**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35332	O-MIC-WIND-250723/3850
N/A	11-Jul-2023	6.7	Active Template Library Elevation of	https://msrc.microsoft.co	O-MIC-WIND-250723/3851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2023-32055**	m/update-guide/vulnerability/CVE-2023-32055	
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-33164**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33164	O-MIC-WIND-250723/3852
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35314	O-MIC-WIND-250723/3853
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Information Disclosure Vulnerability **CVE ID : CVE-2023-35316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35316	O-MIC-WIND-250723/3854
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35318**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35318	O-MIC-WIND-250723/3855
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35319**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35319	O-MIC-WIND-250723/3856
N/A	11-Jul-2023	6.5	Windows Authentication Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/3857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35329	ability/CVE-2023-35329	
N/A	11-Jul-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35308**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35308	O-MIC-WIND-250723/3858
N/A	11-Jul-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35296**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35296	O-MIC-WIND-250723/3859
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32085**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32085	O-MIC-WIND-250723/3860
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35324	O-MIC-WIND-250723/3861
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35306**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35306	O-MIC-WIND-250723/3862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32039**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32039	O-MIC-WIND-250723/3863
N/A	11-Jul-2023	5.5	Microsoft DirectMusic Information Disclosure Vulnerability **CVE ID : CVE-2023-35341**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35341	O-MIC-WIND-250723/3864
N/A	11-Jul-2023	5.4	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35336**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35336	O-MIC-WIND-250723/3865
Product: windows_10_1607					
Affected Version(s): *					
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32040**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32040	O-MIC-WIND-250723/3866
Affected Version(s): * Up to (excluding) 10.0.14393.6085					
N/A	11-Jul-2023	9.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33154	O-MIC-WIND-250723/3867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-32057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32057	O-MIC-WIND-250723/3868
N/A	11-Jul-2023	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32049	O-MIC-WIND-250723/3869
N/A	11-Jul-2023	8.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-35300**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35300	O-MIC-WIND-250723/3870
N/A	11-Jul-2023	8.8	USB Audio Class System Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35303**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35303	O-MIC-WIND-250723/3871
N/A	11-Jul-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-32038**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32038	O-MIC-WIND-250723/3872
N/A	11-Jul-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35302**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35302	O-MIC-WIND-250723/3873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21756**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21756	O-MIC-WIND-250723/3874
N/A	11-Jul-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35305**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35305	O-MIC-WIND-250723/3875
N/A	11-Jul-2023	7.8	Windows Online Certificate Status Protocol (OCSP) SnapIn Remote Code Execution Vulnerability **CVE ID : CVE-2023-35313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35313	O-MIC-WIND-250723/3876
N/A	11-Jul-2023	7.8	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35320	O-MIC-WIND-250723/3877
N/A	11-Jul-2023	7.8	Microsoft VOLSNAP.SYS Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35312	O-MIC-WIND-250723/3878
N/A	11-Jul-2023	7.8	Windows Transaction Manager Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35328**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35328	O-MIC-WIND-250723/3879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35340**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35340	O-MIC-WIND-250723/3880
N/A	11-Jul-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35299**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35299	O-MIC-WIND-250723/3881
N/A	11-Jul-2023	7.8	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35342**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35342	O-MIC-WIND-250723/3882
N/A	11-Jul-2023	7.8	Windows MSHTML Platform Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32046**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046	O-MIC-WIND-250723/3883
N/A	11-Jul-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35304**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35304	O-MIC-WIND-250723/3884
N/A	11-Jul-2023	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32053	O-MIC-WIND-250723/3885
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/3886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Service Vulnerability **CVE ID : CVE-2023-32034**	ability/CVE-2023-32034	
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32035**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32035	O-MIC-WIND-250723/3887
N/A	11-Jul-2023	7.5	OLE Automation Information Disclosure Vulnerability **CVE ID : CVE-2023-32042**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32042	O-MIC-WIND-250723/3888
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32044**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32044	O-MIC-WIND-250723/3889
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32045**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32045	O-MIC-WIND-250723/3890
N/A	11-Jul-2023	7.5	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-35297**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35297	O-MIC-WIND-250723/3891
N/A	11-Jul-2023	7.5	Windows Print Spooler Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/3892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35325	ability/CVE-2023-35325	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	7.5	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35309**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35309	O-MIC-WIND-250723/3893
N/A	11-Jul-2023	7.5	Windows Extended Negotiation Denial of Service Vulnerability **CVE ID : CVE-2023-35330**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35330	O-MIC-WIND-250723/3894
N/A	11-Jul-2023	7.5	Windows Peer Name Resolution Protocol Denial of Service Vulnerability **CVE ID : CVE-2023-35338**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35338	O-MIC-WIND-250723/3895
N/A	11-Jul-2023	7.5	Windows CryptoAPI Denial of Service Vulnerability **CVE ID : CVE-2023-35339**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35339	O-MIC-WIND-250723/3896
N/A	11-Jul-2023	7.4	Windows Netlogon Information Disclosure Vulnerability **CVE ID : CVE-2023-21526**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21526	O-MIC-WIND-250723/3897
N/A	11-Jul-2023	7.3	Volume Shadow Copy Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/3898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32054	ability/CVE-2023-32054	
N/A	11-Jul-2023	6.8	Windows Remote Desktop Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32043	O-MIC-WIND-250723/3899
N/A	11-Jul-2023	6.8	Windows Remote Desktop Protocol Security Feature Bypass **CVE ID : CVE-2023-35332**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35332	O-MIC-WIND-250723/3900
N/A	11-Jul-2023	6.7	Active Template Library Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32055	O-MIC-WIND-250723/3901
N/A	11-Jul-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35296**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35296	O-MIC-WIND-250723/3902
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35314	O-MIC-WIND-250723/3903
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35316	O-MIC-WIND-250723/3904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35316		
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35318**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35318	O-MIC-WIND-250723/3905
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35319**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35319	O-MIC-WIND-250723/3906
N/A	11-Jul-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35308**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35308	O-MIC-WIND-250723/3907
N/A	11-Jul-2023	6.5	Windows Authentication Denial of Service Vulnerability **CVE ID : CVE-2023-35329**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35329	O-MIC-WIND-250723/3908
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-33164**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33164	O-MIC-WIND-250723/3909
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32039**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32039	O-MIC-WIND-250723/3910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	5.5	Windows Update Orchestrator Service Information Disclosure Vulnerability **CVE ID : CVE-2023-32041**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32041	O-MIC-WIND-250723/3911
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32085**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32085	O-MIC-WIND-250723/3912
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35306**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35306	O-MIC-WIND-250723/3913
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35324	O-MIC-WIND-250723/3914
N/A	11-Jul-2023	5.5	Microsoft DirectMusic Information Disclosure Vulnerability **CVE ID : CVE-2023-35341**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35341	O-MIC-WIND-250723/3915
N/A	11-Jul-2023	5.4	Windows MSHTML Platform Security	https://msrc.microsoft.com/update-	O-MIC-WIND-250723/3916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Feature Bypass Vulnerability **CVE ID : CVE-2023-35336**	guide/vulnerability/CVE-2023-35336	
Product: windows_10_1809					
Affected Version(s): *					
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32040**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32040	O-MIC-WIND-250723/3917
Affected Version(s): * Up to (excluding) 10.0.17763.4645					
N/A	11-Jul-2023	9.8	Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32056	O-MIC-WIND-250723/3918
N/A	11-Jul-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-32057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32057	O-MIC-WIND-250723/3919
N/A	11-Jul-2023	9.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33154	O-MIC-WIND-250723/3920
N/A	11-Jul-2023	8.8	USB Audio Class System Driver Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/3921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35303	ability/CVE-2023-35303	
N/A	11-Jul-2023	8.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-35300**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35300	O-MIC-WIND-250723/3922
N/A	11-Jul-2023	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32049	O-MIC-WIND-250723/3923
N/A	11-Jul-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-32038**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32038	O-MIC-WIND-250723/3924
N/A	11-Jul-2023	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35315**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35315	O-MIC-WIND-250723/3925
N/A	11-Jul-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35302**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35302	O-MIC-WIND-250723/3926
N/A	11-Jul-2023	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32053**	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/3927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ability/CVE-2023-32053	
N/A	11-Jul-2023	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21756**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21756	O-MIC-WIND-250723/3928
N/A	11-Jul-2023	7.8	Windows Transaction Manager Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35328**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35328	O-MIC-WIND-250723/3929
N/A	11-Jul-2023	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35340**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35340	O-MIC-WIND-250723/3930
N/A	11-Jul-2023	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33155**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33155	O-MIC-WIND-250723/3931
N/A	11-Jul-2023	7.8	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35342**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35342	O-MIC-WIND-250723/3932
N/A	11-Jul-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35299**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35299	O-MIC-WIND-250723/3933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	7.8	Windows Geolocation Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-35343**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35343	O-MIC-WIND-250723/3934
N/A	11-Jul-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35304**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35304	O-MIC-WIND-250723/3935
N/A	11-Jul-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35305**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35305	O-MIC-WIND-250723/3936
N/A	11-Jul-2023	7.8	Windows MSHTML Platform Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32046**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046	O-MIC-WIND-250723/3937
N/A	11-Jul-2023	7.8	Microsoft VOLSNAP.SYS Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35312	O-MIC-WIND-250723/3938
N/A	11-Jul-2023	7.8	Windows Online Certificate Status Protocol (OCSP) SnapIn Remote Code Execution Vulnerability **CVE ID : CVE-2023-35313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35313	O-MIC-WIND-250723/3939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	7.8	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35320	O-MIC-WIND-250723/3940
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32034	O-MIC-WIND-250723/3941
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32035**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32035	O-MIC-WIND-250723/3942
N/A	11-Jul-2023	7.5	Windows Extended Negotiation Denial of Service Vulnerability **CVE ID : CVE-2023-35330**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35330	O-MIC-WIND-250723/3943
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	7.5	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35309**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35309	O-MIC-WIND-250723/3944
N/A	11-Jul-2023	7.5	OLE Automation Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/3945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32042	ability/CVE-2023-32042	
N/A	11-Jul-2023	7.5	Windows Print Spooler Information Disclosure Vulnerability **CVE ID : CVE-2023-35325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35325	O-MIC-WIND-250723/3946
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32044**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32044	O-MIC-WIND-250723/3947
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32045**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32045	O-MIC-WIND-250723/3948
N/A	11-Jul-2023	7.5	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-35297**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35297	O-MIC-WIND-250723/3949
N/A	11-Jul-2023	7.5	Windows CryptoAPI Denial of Service Vulnerability **CVE ID : CVE-2023-35339**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35339	O-MIC-WIND-250723/3950
N/A	11-Jul-2023	7.5	HTTP.sys Denial of Service Vulnerability **CVE ID : CVE-2023-32084**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32084	O-MIC-WIND-250723/3951
N/A	11-Jul-2023	7.5	Windows Peer Name Resolution Protocol	https://msrc.microsoft.co	O-MIC-WIND-250723/3952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service Vulnerability **CVE ID : CVE-2023-35338**	m/update-guide/vulnerability/CVE-2023-35338	
N/A	11-Jul-2023	7.4	Windows Netlogon Information Disclosure Vulnerability **CVE ID : CVE-2023-21526**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21526	O-MIC-WIND-250723/3953
N/A	11-Jul-2023	7.3	Volume Shadow Copy Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32054	O-MIC-WIND-250723/3954
N/A	11-Jul-2023	6.8	Windows Remote Desktop Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32043	O-MIC-WIND-250723/3955
N/A	11-Jul-2023	6.8	Windows Remote Desktop Protocol Security Feature Bypass **CVE ID : CVE-2023-35332**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35332	O-MIC-WIND-250723/3956
N/A	11-Jul-2023	6.7	Active Template Library Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32055	O-MIC-WIND-250723/3957
N/A	11-Jul-2023	6.5	Windows Layer-2 Bridge Network Driver Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32037	O-MIC-WIND-250723/3958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32037		
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35319**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35319	O-MIC-WIND-250723/3959
N/A	11-Jul-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35308**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35308	O-MIC-WIND-250723/3960
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Information Disclosure Vulnerability **CVE ID : CVE-2023-35316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35316	O-MIC-WIND-250723/3961
N/A	11-Jul-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35296**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35296	O-MIC-WIND-250723/3962
N/A	11-Jul-2023	6.5	Windows Authentication Denial of Service Vulnerability **CVE ID : CVE-2023-35329**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35329	O-MIC-WIND-250723/3963
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/3964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35314	ability/CVE-2023-35314	
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-33164**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33164	O-MIC-WIND-250723/3965
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35318**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35318	O-MIC-WIND-250723/3966
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32039**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32039	O-MIC-WIND-250723/3967
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35324	O-MIC-WIND-250723/3968
N/A	11-Jul-2023	5.5	Windows CDP User Components Information Disclosure Vulnerability **CVE ID : CVE-2023-35326**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35326	O-MIC-WIND-250723/3969
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver	https://msrc.microsoft.com/update-	O-MIC-WIND-250723/3970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability **CVE ID : CVE-2023-32085**	guide/vulnerability/CVE-2023-32085	
N/A	11-Jul-2023	5.5	Windows Update Orchestrator Service Information Disclosure Vulnerability **CVE ID : CVE-2023-32041**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32041	O-MIC-WIND-250723/3971
N/A	11-Jul-2023	5.5	Microsoft DirectMusic Information Disclosure Vulnerability **CVE ID : CVE-2023-35341**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35341	O-MIC-WIND-250723/3972
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35306**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35306	O-MIC-WIND-250723/3973
N/A	11-Jul-2023	5.4	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35336**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35336	O-MIC-WIND-250723/3974
Product: windows_10_21h2					
Affected Version(s): -					
N/A	11-Jul-2023	7.8	Raw Image Extension Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/3975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32051	ability/CVE-2023-32051	
Affected Version(s): *					
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32040**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32040	O-MIC-WIND-250723/3976
Affected Version(s): * Up to (excluding) 10.0.19041.3208					
N/A	11-Jul-2023	9.8	Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32056	O-MIC-WIND-250723/3977
N/A	11-Jul-2023	9.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33154	O-MIC-WIND-250723/3978
N/A	11-Jul-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-32057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32057	O-MIC-WIND-250723/3979
N/A	11-Jul-2023	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32049	O-MIC-WIND-250723/3980
N/A	11-Jul-2023	8.8	USB Audio Class System Driver Remote Code	https://msrc.microsoft.com/update-	O-MIC-WIND-250723/3981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-35303**	guide/vulnerability/CVE-2023-35303	
N/A	11-Jul-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-32038**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32038	O-MIC-WIND-250723/3982
N/A	11-Jul-2023	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35315**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35315	O-MIC-WIND-250723/3983
N/A	11-Jul-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35302**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35302	O-MIC-WIND-250723/3984
N/A	11-Jul-2023	8.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-35300**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35300	O-MIC-WIND-250723/3985
N/A	11-Jul-2023	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21756**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21756	O-MIC-WIND-250723/3986
N/A	11-Jul-2023	7.8	Windows Geolocation Service Remote Code	https://msrc.microsoft.com/update-	O-MIC-WIND-250723/3987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-35343**	guide/vulnerability/CVE-2023-35343	
N/A	11-Jul-2023	7.8	Windows Transaction Manager Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35328**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35328	O-MIC-WIND-250723/3988
N/A	11-Jul-2023	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35337**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35337	O-MIC-WIND-250723/3989
N/A	11-Jul-2023	7.8	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35320	O-MIC-WIND-250723/3990
N/A	11-Jul-2023	7.8	Windows MSHTML Platform Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32046**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046	O-MIC-WIND-250723/3991
N/A	11-Jul-2023	7.8	Windows Online Certificate Status Protocol (OCSP) SnapIn Remote Code Execution Vulnerability **CVE ID : CVE-2023-35313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35313	O-MIC-WIND-250723/3992
N/A	11-Jul-2023	7.8	Microsoft VOLSNAP.SYS	https://msrc.microsoft.com/update-	O-MIC-WIND-250723/3993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35312**	guide/vulnerability/CVE-2023-35312	
N/A	11-Jul-2023	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32053	O-MIC-WIND-250723/3994
N/A	11-Jul-2023	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33155**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33155	O-MIC-WIND-250723/3995
N/A	11-Jul-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35304**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35304	O-MIC-WIND-250723/3996
N/A	11-Jul-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35305**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35305	O-MIC-WIND-250723/3997
N/A	11-Jul-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35299**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35299	O-MIC-WIND-250723/3998
N/A	11-Jul-2023	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35340	O-MIC-WIND-250723/3999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35340		
N/A	11-Jul-2023	7.8	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35342**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35342	O-MIC-WIND-250723/4000
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32034	O-MIC-WIND-250723/4001
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32045**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32045	O-MIC-WIND-250723/4002
N/A	11-Jul-2023	7.5	OLE Automation Information Disclosure Vulnerability **CVE ID : CVE-2023-32042**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32042	O-MIC-WIND-250723/4003
N/A	11-Jul-2023	7.5	Windows Print Spooler Information Disclosure Vulnerability **CVE ID : CVE-2023-35325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35325	O-MIC-WIND-250723/4004
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32035**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32035	O-MIC-WIND-250723/4005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	7.5	Windows Extended Negotiation Denial of Service Vulnerability **CVE ID : CVE-2023-35330**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35330	O-MIC-WIND-250723/4006
N/A	11-Jul-2023	7.5	Windows Peer Name Resolution Protocol Denial of Service Vulnerability **CVE ID : CVE-2023-35338**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35338	O-MIC-WIND-250723/4007
N/A	11-Jul-2023	7.5	Windows CryptoAPI Denial of Service Vulnerability **CVE ID : CVE-2023-35339**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35339	O-MIC-WIND-250723/4008
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	7.5	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35309**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35309	O-MIC-WIND-250723/4009
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32044**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32044	O-MIC-WIND-250723/4010
N/A	11-Jul-2023	7.5	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35297	O-MIC-WIND-250723/4011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35297		
N/A	11-Jul-2023	7.4	Windows Netlogon Information Disclosure Vulnerability **CVE ID : CVE-2023-21526**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21526	O-MIC-WIND-250723/4012
N/A	11-Jul-2023	7.3	Volume Shadow Copy Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32054	O-MIC-WIND-250723/4013
N/A	11-Jul-2023	7.1	Microsoft Install Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35347**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35347	O-MIC-WIND-250723/4014
N/A	11-Jul-2023	6.8	Windows Remote Desktop Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32043	O-MIC-WIND-250723/4015
N/A	11-Jul-2023	6.8	Windows Remote Desktop Protocol Security Feature Bypass **CVE ID : CVE-2023-35332**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35332	O-MIC-WIND-250723/4016
N/A	11-Jul-2023	6.7	Active Template Library Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32055	O-MIC-WIND-250723/4017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35314	O-MIC-WIND-250723/4018
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Information Disclosure Vulnerability **CVE ID : CVE-2023-35316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35316	O-MIC-WIND-250723/4019
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35318**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35318	O-MIC-WIND-250723/4020
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35319**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35319	O-MIC-WIND-250723/4021
N/A	11-Jul-2023	6.5	Windows Layer-2 Bridge Network Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32037**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32037	O-MIC-WIND-250723/4022
N/A	11-Jul-2023	6.5	Windows Authentication Denial of Service Vulnerability **CVE ID : CVE-2023-35329**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35329	O-MIC-WIND-250723/4023
N/A	11-Jul-2023	6.5	Microsoft PostScript and PCL6 Class	https://msrc.microsoft.co	O-MIC-WIND-250723/4024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35296**	m/update-guide/vulnerability/CVE-2023-35296	
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-33164**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33164	O-MIC-WIND-250723/4025
N/A	11-Jul-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35308**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35308	O-MIC-WIND-250723/4026
N/A	11-Jul-2023	5.5	Windows Update Orchestrator Service Information Disclosure Vulnerability **CVE ID : CVE-2023-32041**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32041	O-MIC-WIND-250723/4027
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35324	O-MIC-WIND-250723/4028
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32039	O-MIC-WIND-250723/4029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32039		
N/A	11-Jul-2023	5.5	Windows CDP User Components Information Disclosure Vulnerability **CVE ID : CVE-2023-35326**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35326	O-MIC-WIND-250723/4030
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35306**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35306	O-MIC-WIND-250723/4031
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32085**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32085	O-MIC-WIND-250723/4032
N/A	11-Jul-2023	5.5	Microsoft DirectMusic Information Disclosure Vulnerability **CVE ID : CVE-2023-35341**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35341	O-MIC-WIND-250723/4033
N/A	11-Jul-2023	5.4	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35336**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35336	O-MIC-WIND-250723/4034
Product: windows_10_22h2					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	7.8	Raw Image Extension Remote Code Execution Vulnerability **CVE ID : CVE-2023-32051**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32051	O-MIC-WIND-250723/4035
Affected Version(s): *					
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32040**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32040	O-MIC-WIND-250723/4036
Affected Version(s): * Up to (excluding) 10.0.19045.3208					
N/A	11-Jul-2023	9.8	Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32056	O-MIC-WIND-250723/4037
N/A	11-Jul-2023	9.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33154	O-MIC-WIND-250723/4038
N/A	11-Jul-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-32057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32057	O-MIC-WIND-250723/4039
N/A	11-Jul-2023	8.8	Windows SmartScreen Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32049	ability/CVE-2023-32049	
N/A	11-Jul-2023	8.8	USB Audio Class System Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35303**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35303	O-MIC-WIND-250723/4041
N/A	11-Jul-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-32038**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32038	O-MIC-WIND-250723/4042
N/A	11-Jul-2023	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35315**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35315	O-MIC-WIND-250723/4043
N/A	11-Jul-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35302**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35302	O-MIC-WIND-250723/4044
N/A	11-Jul-2023	8.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-35300**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35300	O-MIC-WIND-250723/4045
N/A	11-Jul-2023	7.8	Windows Win32k Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21756	ability/CVE-2023-21756	
N/A	11-Jul-2023	7.8	Windows Geolocation Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-35343**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35343	O-MIC-WIND-250723/4047
N/A	11-Jul-2023	7.8	Windows Transaction Manager Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35328**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35328	O-MIC-WIND-250723/4048
N/A	11-Jul-2023	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35337**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35337	O-MIC-WIND-250723/4049
N/A	11-Jul-2023	7.8	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35320	O-MIC-WIND-250723/4050
N/A	11-Jul-2023	7.8	Windows MSHTML Platform Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32046**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046	O-MIC-WIND-250723/4051
N/A	11-Jul-2023	7.8	Windows Online Certificate Status Protocol (OCSP) SnapIn Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35313	O-MIC-WIND-250723/4052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35313		
N/A	11-Jul-2023	7.8	Microsoft VOLSNAP.SYS Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35312	O-MIC-WIND-250723/4053
N/A	11-Jul-2023	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32053	O-MIC-WIND-250723/4054
N/A	11-Jul-2023	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33155**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33155	O-MIC-WIND-250723/4055
N/A	11-Jul-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35304**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35304	O-MIC-WIND-250723/4056
N/A	11-Jul-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35305**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35305	O-MIC-WIND-250723/4057
N/A	11-Jul-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35299**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35299	O-MIC-WIND-250723/4058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35340**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35340	O-MIC-WIND-250723/4059
N/A	11-Jul-2023	7.8	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35342**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35342	O-MIC-WIND-250723/4060
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32034	O-MIC-WIND-250723/4061
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32045**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32045	O-MIC-WIND-250723/4062
N/A	11-Jul-2023	7.5	OLE Automation Information Disclosure Vulnerability **CVE ID : CVE-2023-32042**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32042	O-MIC-WIND-250723/4063
N/A	11-Jul-2023	7.5	Windows Print Spooler Information Disclosure Vulnerability **CVE ID : CVE-2023-35325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35325	O-MIC-WIND-250723/4064
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32035	ability/CVE-2023-32035	
N/A	11-Jul-2023	7.5	Windows Extended Negotiation Denial of Service Vulnerability **CVE ID : CVE-2023-35330**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35330	O-MIC-WIND-250723/4066
N/A	11-Jul-2023	7.5	Windows Peer Name Resolution Protocol Denial of Service Vulnerability **CVE ID : CVE-2023-35338**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35338	O-MIC-WIND-250723/4067
N/A	11-Jul-2023	7.5	Windows CryptoAPI Denial of Service Vulnerability **CVE ID : CVE-2023-35339**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35339	O-MIC-WIND-250723/4068
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	7.5	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35309**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35309	O-MIC-WIND-250723/4069
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32044**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32044	O-MIC-WIND-250723/4070
N/A	11-Jul-2023	7.5	Windows Pragmatic General Multicast (PGM) Remote Code	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-35297**	ability/CVE-2023-35297	
N/A	11-Jul-2023	7.4	Windows Netlogon Information Disclosure Vulnerability **CVE ID : CVE-2023-21526**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21526	O-MIC-WIND-250723/4072
N/A	11-Jul-2023	7.3	Volume Shadow Copy Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32054	O-MIC-WIND-250723/4073
N/A	11-Jul-2023	7.1	Microsoft Install Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35347**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35347	O-MIC-WIND-250723/4074
N/A	11-Jul-2023	6.8	Windows Remote Desktop Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32043	O-MIC-WIND-250723/4075
N/A	11-Jul-2023	6.8	Windows Remote Desktop Protocol Security Feature Bypass **CVE ID : CVE-2023-35332**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35332	O-MIC-WIND-250723/4076
N/A	11-Jul-2023	6.7	Active Template Library Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32055	O-MIC-WIND-250723/4077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32055		
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35314	O-MIC-WIND-250723/4078
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Information Disclosure Vulnerability **CVE ID : CVE-2023-35316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35316	O-MIC-WIND-250723/4079
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35318**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35318	O-MIC-WIND-250723/4080
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35319**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35319	O-MIC-WIND-250723/4081
N/A	11-Jul-2023	6.5	Windows Layer-2 Bridge Network Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32037**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32037	O-MIC-WIND-250723/4082
N/A	11-Jul-2023	6.5	Windows Authentication Denial of Service Vulnerability **CVE ID : CVE-2023-35329**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35329	O-MIC-WIND-250723/4083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35296**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35296	O-MIC-WIND-250723/4084
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-33164**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33164	O-MIC-WIND-250723/4085
N/A	11-Jul-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35308**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35308	O-MIC-WIND-250723/4086
N/A	11-Jul-2023	5.5	Windows Update Orchestrator Service Information Disclosure Vulnerability **CVE ID : CVE-2023-32041**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32041	O-MIC-WIND-250723/4087
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35324	O-MIC-WIND-250723/4088
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-32039**	ability/CVE-2023-32039	
N/A	11-Jul-2023	5.5	Windows CDP User Components Information Disclosure Vulnerability **CVE ID : CVE-2023-35326**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35326	O-MIC-WIND-250723/4090
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35306**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35306	O-MIC-WIND-250723/4091
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32085**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32085	O-MIC-WIND-250723/4092
N/A	11-Jul-2023	5.5	Microsoft DirectMusic Information Disclosure Vulnerability **CVE ID : CVE-2023-35341**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35341	O-MIC-WIND-250723/4093
N/A	11-Jul-2023	5.4	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35336**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35336	O-MIC-WIND-250723/4094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: windows_11_21h2					
Affected Version(s): -					
N/A	11-Jul-2023	7.8	Raw Image Extension Remote Code Execution Vulnerability **CVE ID : CVE-2023-32051**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32051	O-MIC-WIND-250723/4095
Affected Version(s): *					
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32040**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32040	O-MIC-WIND-250723/4096
Affected Version(s): * Up to (excluding) 10.0.22000.2176					
N/A	11-Jul-2023	9.8	Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32056	O-MIC-WIND-250723/4097
N/A	11-Jul-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-32057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32057	O-MIC-WIND-250723/4098
N/A	11-Jul-2023	9.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33154	O-MIC-WIND-250723/4099
N/A	11-Jul-2023	8.8	USB Audio Class System Driver	https://msrc.microsoft.co	O-MIC-WIND-250723/4100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability **CVE ID : CVE-2023-35303**	m/update-guide/vulnerability/CVE-2023-35303	
N/A	11-Jul-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-32038**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32038	O-MIC-WIND-250723/4101
N/A	11-Jul-2023	8.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-35300**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35300	O-MIC-WIND-250723/4102
N/A	11-Jul-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35302**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35302	O-MIC-WIND-250723/4103
N/A	11-Jul-2023	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32049	O-MIC-WIND-250723/4104
N/A	11-Jul-2023	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35315**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35315	O-MIC-WIND-250723/4105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32053	O-MIC-WIND-250723/4106
N/A	11-Jul-2023	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21756**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21756	O-MIC-WIND-250723/4107
N/A	11-Jul-2023	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33155**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33155	O-MIC-WIND-250723/4108
N/A	11-Jul-2023	7.8	Windows Transaction Manager Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35328**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35328	O-MIC-WIND-250723/4109
N/A	11-Jul-2023	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35337**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35337	O-MIC-WIND-250723/4110
N/A	11-Jul-2023	7.8	Windows Online Certificate Status Protocol (OCSP) SnapIn Remote Code Execution Vulnerability **CVE ID : CVE-2023-35313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35313	O-MIC-WIND-250723/4111
N/A	11-Jul-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-250723/4112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35304	guide/vulnerability/CVE-2023-35304	
N/A	11-Jul-2023	7.8	Windows OLE Remote Code Execution Vulnerability **CVE ID : CVE-2023-35323**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35323	O-MIC-WIND-250723/4113
N/A	11-Jul-2023	7.8	Windows MSHTML Platform Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32046**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046	O-MIC-WIND-250723/4114
N/A	11-Jul-2023	7.8	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35320	O-MIC-WIND-250723/4115
N/A	11-Jul-2023	7.8	Microsoft VOLSNAP.SYS Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35312	O-MIC-WIND-250723/4116
N/A	11-Jul-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35299**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35299	O-MIC-WIND-250723/4117
N/A	11-Jul-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35305**	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ability/CVE-2023-35305	
N/A	11-Jul-2023	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35340**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35340	O-MIC-WIND-250723/4119
N/A	11-Jul-2023	7.8	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35342**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35342	O-MIC-WIND-250723/4120
N/A	11-Jul-2023	7.8	Windows Geolocation Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-35343**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35343	O-MIC-WIND-250723/4121
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32044**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32044	O-MIC-WIND-250723/4122
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32045**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32045	O-MIC-WIND-250723/4123
N/A	11-Jul-2023	7.5	HTTP.sys Denial of Service Vulnerability **CVE ID : CVE-2023-32084**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32084	O-MIC-WIND-250723/4124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	7.5	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-35297**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35297	O-MIC-WIND-250723/4125
N/A	11-Jul-2023	7.5	HTTP.sys Denial of Service Vulnerability **CVE ID : CVE-2023-35298**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35298	O-MIC-WIND-250723/4126
N/A	11-Jul-2023	7.5	Windows Print Spooler Information Disclosure Vulnerability **CVE ID : CVE-2023-35325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35325	O-MIC-WIND-250723/4127
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	7.5	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35309**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35309	O-MIC-WIND-250723/4128
N/A	11-Jul-2023	7.5	Windows Extended Negotiation Denial of Service Vulnerability **CVE ID : CVE-2023-35330**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35330	O-MIC-WIND-250723/4129
N/A	11-Jul-2023	7.5	Windows Peer Name Resolution Protocol Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35338	ability/CVE-2023-35338	
N/A	11-Jul-2023	7.5	Windows CryptoAPI Denial of Service Vulnerability **CVE ID : CVE-2023-35339**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35339	O-MIC-WIND-250723/4131
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32034	O-MIC-WIND-250723/4132
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32035**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32035	O-MIC-WIND-250723/4133
N/A	11-Jul-2023	7.5	OLE Automation Information Disclosure Vulnerability **CVE ID : CVE-2023-32042**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32042	O-MIC-WIND-250723/4134
N/A	11-Jul-2023	7.4	Windows Netlogon Information Disclosure Vulnerability **CVE ID : CVE-2023-21526**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21526	O-MIC-WIND-250723/4135
N/A	11-Jul-2023	7.3	Volume Shadow Copy Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32054	O-MIC-WIND-250723/4136
N/A	11-Jul-2023	7.1	Microsoft Install Service Elevation of	https://msrc.microsoft.co	O-MIC-WIND-250723/4137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2023-35347**	m/update-guide/vulnerability/CVE-2023-35347	
N/A	11-Jul-2023	6.8	Windows Remote Desktop Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32043	O-MIC-WIND-250723/4138
N/A	11-Jul-2023	6.8	Windows Remote Desktop Protocol Security Feature Bypass **CVE ID : CVE-2023-35332**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35332	O-MIC-WIND-250723/4139
N/A	11-Jul-2023	6.7	Active Template Library Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32055	O-MIC-WIND-250723/4140
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35314	O-MIC-WIND-250723/4141
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Information Disclosure Vulnerability **CVE ID : CVE-2023-35316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35316	O-MIC-WIND-250723/4142
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35318	ability/CVE-2023-35318	
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35319**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35319	O-MIC-WIND-250723/4144
N/A	11-Jul-2023	6.5	Windows Layer-2 Bridge Network Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32037**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32037	O-MIC-WIND-250723/4145
N/A	11-Jul-2023	6.5	Windows Authentication Denial of Service Vulnerability **CVE ID : CVE-2023-35329**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35329	O-MIC-WIND-250723/4146
N/A	11-Jul-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35308**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35308	O-MIC-WIND-250723/4147
N/A	11-Jul-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35296**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35296	O-MIC-WIND-250723/4148
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33164	ability/CVE-2023-33164	
N/A	11-Jul-2023	5.5	Windows Update Orchestrator Service Information Disclosure Vulnerability **CVE ID : CVE-2023-32041**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32041	O-MIC-WIND-250723/4150
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35324	O-MIC-WIND-250723/4151
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32039**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32039	O-MIC-WIND-250723/4152
N/A	11-Jul-2023	5.5	Windows CDP User Components Information Disclosure Vulnerability **CVE ID : CVE-2023-35326**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35326	O-MIC-WIND-250723/4153
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32085**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32085	O-MIC-WIND-250723/4154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35306**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35306	O-MIC-WIND-250723/4155
N/A	11-Jul-2023	5.5	Microsoft DirectMusic Information Disclosure Vulnerability **CVE ID : CVE-2023-35341**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35341	O-MIC-WIND-250723/4156
N/A	11-Jul-2023	5.4	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35336**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35336	O-MIC-WIND-250723/4157
Product: windows_11_22h2					
Affected Version(s): -					
N/A	11-Jul-2023	7.8	Raw Image Extension Remote Code Execution Vulnerability **CVE ID : CVE-2023-32051**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32051	O-MIC-WIND-250723/4158
Affected Version(s): *					
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32040**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32040	O-MIC-WIND-250723/4159
Affected Version(s): * Up to (excluding) 10.0.22621.1992					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	9.8	Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32056	O-MIC-WIND-250723/4160
N/A	11-Jul-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-32057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32057	O-MIC-WIND-250723/4161
N/A	11-Jul-2023	9.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33154	O-MIC-WIND-250723/4162
N/A	11-Jul-2023	8.8	USB Audio Class System Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35303**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35303	O-MIC-WIND-250723/4163
N/A	11-Jul-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-32038**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32038	O-MIC-WIND-250723/4164
N/A	11-Jul-2023	8.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-35300**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35300	O-MIC-WIND-250723/4165
N/A	11-Jul-2023	8.8	Microsoft PostScript and PCL6 Class	https://msrc.microsoft.co	O-MIC-WIND-250723/4166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35302**	m/update-guide/vulnerability/CVE-2023-35302	
N/A	11-Jul-2023	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32049	O-MIC-WIND-250723/4167
N/A	11-Jul-2023	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35315**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35315	O-MIC-WIND-250723/4168
N/A	11-Jul-2023	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32053	O-MIC-WIND-250723/4169
N/A	11-Jul-2023	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21756**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21756	O-MIC-WIND-250723/4170
N/A	11-Jul-2023	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33155**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33155	O-MIC-WIND-250723/4171
N/A	11-Jul-2023	7.8	Windows CNG Key Isolation Service	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35340**	ability/CVE-2023-35340	
N/A	11-Jul-2023	7.8	Windows Transaction Manager Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35328**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35328	O-MIC-WIND-250723/4173
N/A	11-Jul-2023	7.8	Windows Online Certificate Status Protocol (OCSP) SnapIn Remote Code Execution Vulnerability **CVE ID : CVE-2023-35313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35313	O-MIC-WIND-250723/4174
N/A	11-Jul-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35304**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35304	O-MIC-WIND-250723/4175
N/A	11-Jul-2023	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35337**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35337	O-MIC-WIND-250723/4176
N/A	11-Jul-2023	7.8	Windows MSHTML Platform Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32046**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046	O-MIC-WIND-250723/4177
N/A	11-Jul-2023	7.8	Connected User Experiences and Telemetry Elevation	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Privilege Vulnerability **CVE ID : CVE-2023-35320**	ability/CVE-2023-35320	
N/A	11-Jul-2023	7.8	Microsoft VOLSNAP.SYS Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35312	O-MIC-WIND-250723/4179
N/A	11-Jul-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35299**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35299	O-MIC-WIND-250723/4180
N/A	11-Jul-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35305**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35305	O-MIC-WIND-250723/4181
N/A	11-Jul-2023	7.8	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35342**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35342	O-MIC-WIND-250723/4182
N/A	11-Jul-2023	7.8	Windows Geolocation Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-35343**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35343	O-MIC-WIND-250723/4183
N/A	11-Jul-2023	7.5	OLE Automation Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32042	ability/CVE-2023-32042	
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32044**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32044	O-MIC-WIND-250723/4185
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32045**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32045	O-MIC-WIND-250723/4186
N/A	11-Jul-2023	7.5	HTTP.sys Denial of Service Vulnerability **CVE ID : CVE-2023-32084**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32084	O-MIC-WIND-250723/4187
N/A	11-Jul-2023	7.5	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-35297**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35297	O-MIC-WIND-250723/4188
N/A	11-Jul-2023	7.5	HTTP.sys Denial of Service Vulnerability **CVE ID : CVE-2023-35298**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35298	O-MIC-WIND-250723/4189
N/A	11-Jul-2023	7.5	Windows Print Spooler Information Disclosure Vulnerability **CVE ID : CVE-2023-35325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35325	O-MIC-WIND-250723/4190
Concurrent Execution	11-Jul-2023	7.5	Microsoft Message Queuing Remote	https://msrc.microsoft.co	O-MIC-WIND-250723/4191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			Code Execution Vulnerability **CVE ID : CVE-2023-35309**	m/update-guide/vulnerability/CVE-2023-35309	
N/A	11-Jul-2023	7.5	Windows Extended Negotiation Denial of Service Vulnerability **CVE ID : CVE-2023-35330**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35330	O-MIC-WIND-250723/4192
N/A	11-Jul-2023	7.5	Windows Peer Name Resolution Protocol Denial of Service Vulnerability **CVE ID : CVE-2023-35338**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35338	O-MIC-WIND-250723/4193
N/A	11-Jul-2023	7.5	Windows CryptoAPI Denial of Service Vulnerability **CVE ID : CVE-2023-35339**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35339	O-MIC-WIND-250723/4194
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32034	O-MIC-WIND-250723/4195
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32035**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32035	O-MIC-WIND-250723/4196
N/A	11-Jul-2023	7.4	Windows Netlogon Information	https://msrc.microsoft.co	O-MIC-WIND-250723/4197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-21526**	m/update-guide/vulnerability/CVE-2023-21526	
N/A	11-Jul-2023	7.3	Volume Shadow Copy Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32054	O-MIC-WIND-250723/4198
N/A	11-Jul-2023	7.1	Microsoft Install Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35347**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35347	O-MIC-WIND-250723/4199
N/A	11-Jul-2023	6.8	Windows Remote Desktop Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32043	O-MIC-WIND-250723/4200
N/A	11-Jul-2023	6.8	Windows Remote Desktop Protocol Security Feature Bypass **CVE ID : CVE-2023-35332**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35332	O-MIC-WIND-250723/4201
N/A	11-Jul-2023	6.7	Active Template Library Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32055	O-MIC-WIND-250723/4202
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33164	O-MIC-WIND-250723/4203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33164		
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35314	O-MIC-WIND-250723/4204
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Information Disclosure Vulnerability **CVE ID : CVE-2023-35316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35316	O-MIC-WIND-250723/4205
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35318**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35318	O-MIC-WIND-250723/4206
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35319**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35319	O-MIC-WIND-250723/4207
N/A	11-Jul-2023	6.5	Windows Authentication Denial of Service Vulnerability **CVE ID : CVE-2023-35329**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35329	O-MIC-WIND-250723/4208
N/A	11-Jul-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35308**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35308	O-MIC-WIND-250723/4209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	6.5	Windows Layer-2 Bridge Network Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32037**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32037	O-MIC-WIND-250723/4210
N/A	11-Jul-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35296**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35296	O-MIC-WIND-250723/4211
N/A	11-Jul-2023	5.5	Windows Update Orchestrator Service Information Disclosure Vulnerability **CVE ID : CVE-2023-32041**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32041	O-MIC-WIND-250723/4212
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35324	O-MIC-WIND-250723/4213
N/A	11-Jul-2023	5.5	Windows CDP User Components Information Disclosure Vulnerability **CVE ID : CVE-2023-35326**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35326	O-MIC-WIND-250723/4214
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-32039**	ability/CVE-2023-32039	
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32085**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32085	O-MIC-WIND-250723/4216
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35306**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35306	O-MIC-WIND-250723/4217
N/A	11-Jul-2023	5.5	Microsoft DirectMusic Information Disclosure Vulnerability **CVE ID : CVE-2023-35341**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35341	O-MIC-WIND-250723/4218
N/A	11-Jul-2023	5.4	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35336**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35336	O-MIC-WIND-250723/4219
Product: windows_server_2008					
Affected Version(s): -					
N/A	11-Jul-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32057	ability/CVE-2023-32057	
N/A	11-Jul-2023	9.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33154	O-MIC-WIND-250723/4221
N/A	11-Jul-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-32038**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32038	O-MIC-WIND-250723/4222
N/A	11-Jul-2023	8.8	Windows Deployment Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-35322**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35322	O-MIC-WIND-250723/4223
N/A	11-Jul-2023	8.8	USB Audio Class System Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35303**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35303	O-MIC-WIND-250723/4224
N/A	11-Jul-2023	8.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-35300**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35300	O-MIC-WIND-250723/4225
N/A	11-Jul-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35299	O-MIC-WIND-250723/4226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35299		
N/A	11-Jul-2023	7.8	Windows Transaction Manager Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35328**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35328	O-MIC-WIND-250723/4227
N/A	11-Jul-2023	7.8	Windows MSHTML Platform Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32046**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046	O-MIC-WIND-250723/4228
N/A	11-Jul-2023	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35340**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35340	O-MIC-WIND-250723/4229
N/A	11-Jul-2023	7.5	Windows Peer Name Resolution Protocol Denial of Service Vulnerability **CVE ID : CVE-2023-35338**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35338	O-MIC-WIND-250723/4230
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32034	O-MIC-WIND-250723/4231
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32035**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32035	O-MIC-WIND-250723/4232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	7.5	OLE Automation Information Disclosure Vulnerability **CVE ID : CVE-2023-32042**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32042	O-MIC-WIND-250723/4233
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32044**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32044	O-MIC-WIND-250723/4234
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32045**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32045	O-MIC-WIND-250723/4235
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	7.5	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35309**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35309	O-MIC-WIND-250723/4236
N/A	11-Jul-2023	7.5	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-35297**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35297	O-MIC-WIND-250723/4237
N/A	11-Jul-2023	7.4	Windows Netlogon Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21526	ability/CVE-2023-21526	
N/A	11-Jul-2023	7.2	Microsoft Failover Cluster Remote Code Execution Vulnerability **CVE ID : CVE-2023-32033**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32033	O-MIC-WIND-250723/4239
N/A	11-Jul-2023	7.2	Windows Active Directory Certificate Services (AD CS) Remote Code Execution Vulnerability **CVE ID : CVE-2023-35350**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35350	O-MIC-WIND-250723/4240
N/A	11-Jul-2023	7	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32050**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32050	O-MIC-WIND-250723/4241
N/A	11-Jul-2023	6.8	Windows Remote Desktop Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32043	O-MIC-WIND-250723/4242
N/A	11-Jul-2023	6.7	Active Template Library Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32055	O-MIC-WIND-250723/4243
Concurrent Execution using Shared Resource with Improper	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35310**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35310	O-MIC-WIND-250723/4244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')					
N/A	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35344**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35344	O-MIC-WIND-250723/4245
N/A	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35345**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35345	O-MIC-WIND-250723/4246
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35346**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35346	O-MIC-WIND-250723/4247
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-33164**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33164	O-MIC-WIND-250723/4248
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35314	O-MIC-WIND-250723/4249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Information Disclosure Vulnerability **CVE ID : CVE-2023-35316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35316	O-MIC-WIND-250723/4250
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35318**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35318	O-MIC-WIND-250723/4251
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35319**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35319	O-MIC-WIND-250723/4252
N/A	11-Jul-2023	6.5	Windows Deployment Services Denial of Service Vulnerability **CVE ID : CVE-2023-35321**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35321	O-MIC-WIND-250723/4253
N/A	11-Jul-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35296**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35296	O-MIC-WIND-250723/4254
Affected Version(s): r2					
N/A	11-Jul-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-32057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32057	O-MIC-WIND-250723/4255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	9.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33154	O-MIC-WIND-250723/4256
N/A	11-Jul-2023	8.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-35300**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35300	O-MIC-WIND-250723/4257
N/A	11-Jul-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-32038**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32038	O-MIC-WIND-250723/4258
N/A	11-Jul-2023	8.8	Windows Deployment Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-35322**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35322	O-MIC-WIND-250723/4259
N/A	11-Jul-2023	8.8	USB Audio Class System Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35303**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35303	O-MIC-WIND-250723/4260
N/A	11-Jul-2023	7.8	Windows Transaction Manager Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35328**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35328	O-MIC-WIND-250723/4261
N/A	11-Jul-2023	7.8	Windows MSHTML Platform Elevation of	https://msrc.microsoft.co	O-MIC-WIND-250723/4262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2023-32046**	m/update-guide/vulnerability/CVE-2023-32046	
N/A	11-Jul-2023	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32053	O-MIC-WIND-250723/4263
N/A	11-Jul-2023	7.8	Microsoft VOLSNAP.SYS Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35312	O-MIC-WIND-250723/4264
N/A	11-Jul-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35299**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35299	O-MIC-WIND-250723/4265
N/A	11-Jul-2023	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35340**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35340	O-MIC-WIND-250723/4266
N/A	11-Jul-2023	7.8	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35342**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35342	O-MIC-WIND-250723/4267
N/A	11-Jul-2023	7.5	OLE Automation Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32042	ability/CVE-2023-32042	
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32034	O-MIC-WIND-250723/4269
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32035**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32035	O-MIC-WIND-250723/4270
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32044**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32044	O-MIC-WIND-250723/4271
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32045**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32045	O-MIC-WIND-250723/4272
N/A	11-Jul-2023	7.5	Windows Network Load Balancing Remote Code Execution Vulnerability **CVE ID : CVE-2023-33163**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33163	O-MIC-WIND-250723/4273
Concurrent Execution using Shared Resource with Improper Synchroniz	11-Jul-2023	7.5	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35309**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35309	O-MIC-WIND-250723/4274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')					
N/A	11-Jul-2023	7.5	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-35297**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35297	O-MIC-WIND-250723/4275
N/A	11-Jul-2023	7.5	Windows Extended Negotiation Denial of Service Vulnerability **CVE ID : CVE-2023-35330**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35330	O-MIC-WIND-250723/4276
N/A	11-Jul-2023	7.5	Windows Peer Name Resolution Protocol Denial of Service Vulnerability **CVE ID : CVE-2023-35338**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35338	O-MIC-WIND-250723/4277
N/A	11-Jul-2023	7.4	Windows Netlogon Information Disclosure Vulnerability **CVE ID : CVE-2023-21526**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21526	O-MIC-WIND-250723/4278
N/A	11-Jul-2023	7.2	Microsoft Failover Cluster Remote Code Execution Vulnerability **CVE ID : CVE-2023-32033**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32033	O-MIC-WIND-250723/4279
N/A	11-Jul-2023	7.2	Windows Active Directory Certificate Services (AD CS) Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35350	O-MIC-WIND-250723/4280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35350		
N/A	11-Jul-2023	7	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32050**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32050	O-MIC-WIND-250723/4281
N/A	11-Jul-2023	6.8	Windows Remote Desktop Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32043	O-MIC-WIND-250723/4282
N/A	11-Jul-2023	6.8	Windows Remote Desktop Protocol Security Feature Bypass **CVE ID : CVE-2023-35332**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35332	O-MIC-WIND-250723/4283
N/A	11-Jul-2023	6.7	Active Template Library Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32055	O-MIC-WIND-250723/4284
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35310**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35310	O-MIC-WIND-250723/4285
N/A	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35344	ability/CVE-2023-35344	
N/A	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35345**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35345	O-MIC-WIND-250723/4287
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35346**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35346	O-MIC-WIND-250723/4288
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Information Disclosure Vulnerability **CVE ID : CVE-2023-35316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35316	O-MIC-WIND-250723/4289
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35318**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35318	O-MIC-WIND-250723/4290
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35319**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35319	O-MIC-WIND-250723/4291
N/A	11-Jul-2023	6.5	Windows Deployment Services	https://msrc.microsoft.com/update-	O-MIC-WIND-250723/4292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service Vulnerability **CVE ID : CVE-2023-35321**	guide/vulnerability/CVE-2023-35321	
N/A	11-Jul-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35296**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35296	O-MIC-WIND-250723/4293
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-33164**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33164	O-MIC-WIND-250723/4294
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35314	O-MIC-WIND-250723/4295
N/A	11-Jul-2023	5.5	Microsoft DirectMusic Information Disclosure Vulnerability **CVE ID : CVE-2023-35341**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35341	O-MIC-WIND-250723/4296
Product: windows_server_2012					
Affected Version(s): -					
N/A	11-Jul-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-32057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32057	O-MIC-WIND-250723/4297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	9.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33154	O-MIC-WIND-250723/4298
N/A	11-Jul-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-32038**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32038	O-MIC-WIND-250723/4299
N/A	11-Jul-2023	8.8	Windows Deployment Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-35322**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35322	O-MIC-WIND-250723/4300
N/A	11-Jul-2023	8.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-35300**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35300	O-MIC-WIND-250723/4301
N/A	11-Jul-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35302**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35302	O-MIC-WIND-250723/4302
N/A	11-Jul-2023	8.8	USB Audio Class System Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35303**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35303	O-MIC-WIND-250723/4303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	7.8	Windows MSHTML Platform Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32046**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046	O-MIC-WIND-250723/4304
N/A	11-Jul-2023	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21756**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21756	O-MIC-WIND-250723/4305
N/A	11-Jul-2023	7.8	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35342**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35342	O-MIC-WIND-250723/4306
N/A	11-Jul-2023	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35340**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35340	O-MIC-WIND-250723/4307
N/A	11-Jul-2023	7.8	Windows Transaction Manager Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35328**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35328	O-MIC-WIND-250723/4308
N/A	11-Jul-2023	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32053	O-MIC-WIND-250723/4309
N/A	11-Jul-2023	7.8	Windows Server Update Service (WSUS) Elevation of	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2023-35317**	ability/CVE-2023-35317	
N/A	11-Jul-2023	7.8	Microsoft VOLSNAP.SYS Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35312	O-MIC-WIND-250723/4311
N/A	11-Jul-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35299**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35299	O-MIC-WIND-250723/4312
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32034	O-MIC-WIND-250723/4313
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32035**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32035	O-MIC-WIND-250723/4314
N/A	11-Jul-2023	7.5	Windows Peer Name Resolution Protocol Denial of Service Vulnerability **CVE ID : CVE-2023-35338**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35338	O-MIC-WIND-250723/4315
N/A	11-Jul-2023	7.5	OLE Automation Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32042	ability/CVE-2023-32042	
N/A	11-Jul-2023	7.5	Windows Extended Negotiation Denial of Service Vulnerability **CVE ID : CVE-2023-35330**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35330	O-MIC-WIND-250723/4317
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32044**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32044	O-MIC-WIND-250723/4318
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32045**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32045	O-MIC-WIND-250723/4319
N/A	11-Jul-2023	7.5	Windows Print Spooler Information Disclosure Vulnerability **CVE ID : CVE-2023-35325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35325	O-MIC-WIND-250723/4320
N/A	11-Jul-2023	7.5	Windows Network Load Balancing Remote Code Execution Vulnerability **CVE ID : CVE-2023-33163**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33163	O-MIC-WIND-250723/4321
Concurrent Execution using Shared Resource with Improper Synchroniz	11-Jul-2023	7.5	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35309**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35309	O-MIC-WIND-250723/4322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')					
N/A	11-Jul-2023	7.5	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-35297**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35297	O-MIC-WIND-250723/4323
N/A	11-Jul-2023	7.4	Windows Netlogon Information Disclosure Vulnerability **CVE ID : CVE-2023-21526**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21526	O-MIC-WIND-250723/4324
N/A	11-Jul-2023	7.3	Volume Shadow Copy Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32054	O-MIC-WIND-250723/4325
N/A	11-Jul-2023	7.2	Microsoft Failover Cluster Remote Code Execution Vulnerability **CVE ID : CVE-2023-32033**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32033	O-MIC-WIND-250723/4326
N/A	11-Jul-2023	7.2	Windows Active Directory Certificate Services (AD CS) Remote Code Execution Vulnerability **CVE ID : CVE-2023-35350**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35350	O-MIC-WIND-250723/4327
N/A	11-Jul-2023	6.8	Windows Remote Desktop Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32043	ability/CVE-2023-32043	
N/A	11-Jul-2023	6.8	Windows Remote Desktop Protocol Security Feature Bypass **CVE ID : CVE-2023-35332**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35332	O-MIC-WIND-250723/4329
N/A	11-Jul-2023	6.7	Active Template Library Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32055	O-MIC-WIND-250723/4330
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35310**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35310	O-MIC-WIND-250723/4331
N/A	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35344**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35344	O-MIC-WIND-250723/4332
N/A	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35345**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35345	O-MIC-WIND-250723/4333
Concurrent Execution using Shared	11-Jul-2023	6.6	Windows DNS Server Remote Code	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			Execution Vulnerability **CVE ID : CVE-2023-35346**	ability/CVE-2023-35346	
N/A	11-Jul-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35308**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35308	O-MIC-WIND-250723/4335
N/A	11-Jul-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35296**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35296	O-MIC-WIND-250723/4336
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-33164**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33164	O-MIC-WIND-250723/4337
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35314	O-MIC-WIND-250723/4338
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35318**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35318	O-MIC-WIND-250723/4339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35319**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35319	O-MIC-WIND-250723/4340
N/A	11-Jul-2023	6.5	Windows Deployment Services Denial of Service Vulnerability **CVE ID : CVE-2023-35321**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35321	O-MIC-WIND-250723/4341
N/A	11-Jul-2023	6.5	Windows Authentication Denial of Service Vulnerability **CVE ID : CVE-2023-35329**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35329	O-MIC-WIND-250723/4342
N/A	11-Jul-2023	6.5	Windows Local Security Authority (LSA) Denial of Service Vulnerability **CVE ID : CVE-2023-35331**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35331	O-MIC-WIND-250723/4343
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Information Disclosure Vulnerability **CVE ID : CVE-2023-35316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35316	O-MIC-WIND-250723/4344
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35306**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35306	O-MIC-WIND-250723/4345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32085**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32085	O-MIC-WIND-250723/4346
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35324	O-MIC-WIND-250723/4347
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32039**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32039	O-MIC-WIND-250723/4348
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32040**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32040	O-MIC-WIND-250723/4349
N/A	11-Jul-2023	5.5	Microsoft DirectMusic Information Disclosure Vulnerability **CVE ID : CVE-2023-35341**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35341	O-MIC-WIND-250723/4350
Affected Version(s): r2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-32057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32057	O-MIC-WIND-250723/4351
N/A	11-Jul-2023	9.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33154	O-MIC-WIND-250723/4352
N/A	11-Jul-2023	8.8	USB Audio Class System Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35303**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35303	O-MIC-WIND-250723/4353
N/A	11-Jul-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-32038**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32038	O-MIC-WIND-250723/4354
N/A	11-Jul-2023	8.8	Windows Deployment Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-35322**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35322	O-MIC-WIND-250723/4355
N/A	11-Jul-2023	8.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-35300**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35300	O-MIC-WIND-250723/4356
N/A	11-Jul-2023	8.8	Microsoft PostScript and PCL6 Class	https://msrc.microsoft.co	O-MIC-WIND-250723/4357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35302**	m/update-guide/vulnerability/CVE-2023-35302	
N/A	11-Jul-2023	7.8	Windows MSHTML Platform Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32046**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046	O-MIC-WIND-250723/4358
N/A	11-Jul-2023	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21756**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21756	O-MIC-WIND-250723/4359
N/A	11-Jul-2023	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35340**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35340	O-MIC-WIND-250723/4360
N/A	11-Jul-2023	7.8	Windows Transaction Manager Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35328**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35328	O-MIC-WIND-250723/4361
N/A	11-Jul-2023	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32053	O-MIC-WIND-250723/4362
N/A	11-Jul-2023	7.8	Windows Server Update Service (WSUS) Elevation of	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2023-35317**	ability/CVE-2023-35317	
N/A	11-Jul-2023	7.8	Microsoft VOLSNAP.SYS Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35312	O-MIC-WIND-250723/4364
N/A	11-Jul-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35299**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35299	O-MIC-WIND-250723/4365
N/A	11-Jul-2023	7.8	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35342**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35342	O-MIC-WIND-250723/4366
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32034	O-MIC-WIND-250723/4367
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32035**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32035	O-MIC-WIND-250723/4368
N/A	11-Jul-2023	7.5	OLE Automation Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32042	ability/CVE-2023-32042	
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32044**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32044	O-MIC-WIND-250723/4370
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32045**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32045	O-MIC-WIND-250723/4371
N/A	11-Jul-2023	7.5	Windows Print Spooler Information Disclosure Vulnerability **CVE ID : CVE-2023-35325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35325	O-MIC-WIND-250723/4372
N/A	11-Jul-2023	7.5	Windows Network Load Balancing Remote Code Execution Vulnerability **CVE ID : CVE-2023-33163**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33163	O-MIC-WIND-250723/4373
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	7.5	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35309**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35309	O-MIC-WIND-250723/4374
N/A	11-Jul-2023	7.5	Windows Pragmatic General Multicast (PGM) Remote Code	https://msrc.microsoft.com/update-	O-MIC-WIND-250723/4375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-35297**	guide/vulnerability/CVE-2023-35297	
N/A	11-Jul-2023	7.5	Windows Extended Negotiation Denial of Service Vulnerability **CVE ID : CVE-2023-35330**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35330	O-MIC-WIND-250723/4376
N/A	11-Jul-2023	7.5	Windows Peer Name Resolution Protocol Denial of Service Vulnerability **CVE ID : CVE-2023-35338**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35338	O-MIC-WIND-250723/4377
N/A	11-Jul-2023	7.4	Windows Netlogon Information Disclosure Vulnerability **CVE ID : CVE-2023-21526**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21526	O-MIC-WIND-250723/4378
N/A	11-Jul-2023	7.3	Volume Shadow Copy Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32054	O-MIC-WIND-250723/4379
N/A	11-Jul-2023	7.2	Windows Active Directory Certificate Services (AD CS) Remote Code Execution Vulnerability **CVE ID : CVE-2023-35350**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35350	O-MIC-WIND-250723/4380
N/A	11-Jul-2023	7.2	Microsoft Failover Cluster Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32033	ability/CVE-2023-32033	
N/A	11-Jul-2023	6.8	Windows Remote Desktop Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32043	O-MIC-WIND-250723/4382
N/A	11-Jul-2023	6.8	Windows Remote Desktop Protocol Security Feature Bypass **CVE ID : CVE-2023-35332**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35332	O-MIC-WIND-250723/4383
N/A	11-Jul-2023	6.7	Active Template Library Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32055	O-MIC-WIND-250723/4384
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35310**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35310	O-MIC-WIND-250723/4385
N/A	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35344**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35344	O-MIC-WIND-250723/4386
N/A	11-Jul-2023	6.6	Windows DNS Server Remote Code	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-35345**	ability/CVE-2023-35345	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35346**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35346	O-MIC-WIND-250723/4388
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-33164**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33164	O-MIC-WIND-250723/4389
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35314	O-MIC-WIND-250723/4390
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35318**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35318	O-MIC-WIND-250723/4391
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35319**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35319	O-MIC-WIND-250723/4392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	6.5	Windows Deployment Services Denial of Service Vulnerability **CVE ID : CVE-2023-35321**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35321	O-MIC-WIND-250723/4393
N/A	11-Jul-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35308**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35308	O-MIC-WIND-250723/4394
N/A	11-Jul-2023	6.5	Windows Local Security Authority (LSA) Denial of Service Vulnerability **CVE ID : CVE-2023-35331**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35331	O-MIC-WIND-250723/4395
N/A	11-Jul-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35296**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35296	O-MIC-WIND-250723/4396
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Information Disclosure Vulnerability **CVE ID : CVE-2023-35316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35316	O-MIC-WIND-250723/4397
N/A	11-Jul-2023	6.5	Windows Authentication Denial of Service Vulnerability **CVE ID : CVE-2023-35329**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35329	O-MIC-WIND-250723/4398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35306**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35306	O-MIC-WIND-250723/4399
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32085**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32085	O-MIC-WIND-250723/4400
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35324	O-MIC-WIND-250723/4401
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32039**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32039	O-MIC-WIND-250723/4402
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32040**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32040	O-MIC-WIND-250723/4403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	5.5	Microsoft DirectMusic Information Disclosure Vulnerability **CVE ID : CVE-2023-35341**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35341	O-MIC-WIND-250723/4404
N/A	11-Jul-2023	5.4	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35336**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35336	O-MIC-WIND-250723/4405
Product: windows_server_2016					
Affected Version(s): -					
N/A	11-Jul-2023	9.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33154	O-MIC-WIND-250723/4406
N/A	11-Jul-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-32057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32057	O-MIC-WIND-250723/4407
N/A	11-Jul-2023	8.8	USB Audio Class System Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35303**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35303	O-MIC-WIND-250723/4408
N/A	11-Jul-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35302	O-MIC-WIND-250723/4409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35302		
N/A	11-Jul-2023	8.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-35300**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35300	O-MIC-WIND-250723/4410
N/A	11-Jul-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-32038**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32038	O-MIC-WIND-250723/4411
N/A	11-Jul-2023	8.8	Windows Deployment Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-35322**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35322	O-MIC-WIND-250723/4412
N/A	11-Jul-2023	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32049	O-MIC-WIND-250723/4413
N/A	11-Jul-2023	7.8	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35320	O-MIC-WIND-250723/4414
N/A	11-Jul-2023	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21756**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21756	O-MIC-WIND-250723/4415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35299**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35299	O-MIC-WIND-250723/4416
N/A	11-Jul-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35304**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35304	O-MIC-WIND-250723/4417
N/A	11-Jul-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35305**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35305	O-MIC-WIND-250723/4418
N/A	11-Jul-2023	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35340**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35340	O-MIC-WIND-250723/4419
N/A	11-Jul-2023	7.8	Windows Transaction Manager Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35328**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35328	O-MIC-WIND-250723/4420
N/A	11-Jul-2023	7.8	Windows MSHTML Platform Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32046**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046	O-MIC-WIND-250723/4421
N/A	11-Jul-2023	7.8	Windows Installer Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32053	ability/CVE-2023-32053	
N/A	11-Jul-2023	7.8	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35342**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35342	O-MIC-WIND-250723/4423
N/A	11-Jul-2023	7.8	Windows Online Certificate Status Protocol (OCSP) SnapIn Remote Code Execution Vulnerability **CVE ID : CVE-2023-35313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35313	O-MIC-WIND-250723/4424
N/A	11-Jul-2023	7.8	Microsoft VOLSNAP.SYS Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35312	O-MIC-WIND-250723/4425
N/A	11-Jul-2023	7.8	Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35317**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35317	O-MIC-WIND-250723/4426
N/A	11-Jul-2023	7.5	Windows Peer Name Resolution Protocol Denial of Service Vulnerability **CVE ID : CVE-2023-35338**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35338	O-MIC-WIND-250723/4427
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32034	ability/CVE-2023-32034	
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32035**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32035	O-MIC-WIND-250723/4429
N/A	11-Jul-2023	7.5	Windows Extended Negotiation Denial of Service Vulnerability **CVE ID : CVE-2023-35330**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35330	O-MIC-WIND-250723/4430
N/A	11-Jul-2023	7.5	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-35297**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35297	O-MIC-WIND-250723/4431
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32044**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32044	O-MIC-WIND-250723/4432
N/A	11-Jul-2023	7.5	Windows Print Spooler Information Disclosure Vulnerability **CVE ID : CVE-2023-35325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35325	O-MIC-WIND-250723/4433
N/A	11-Jul-2023	7.5	OLE Automation Information Disclosure Vulnerability **CVE ID : CVE-2023-32042**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32042	O-MIC-WIND-250723/4434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	7.5	Windows CryptoAPI Denial of Service Vulnerability **CVE ID : CVE-2023-35339**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35339	O-MIC-WIND-250723/4435
N/A	11-Jul-2023	7.5	Windows Network Load Balancing Remote Code Execution Vulnerability **CVE ID : CVE-2023-33163**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33163	O-MIC-WIND-250723/4436
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	7.5	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35309**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35309	O-MIC-WIND-250723/4437
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32045**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32045	O-MIC-WIND-250723/4438
N/A	11-Jul-2023	7.4	Windows Netlogon Information Disclosure Vulnerability **CVE ID : CVE-2023-21526**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21526	O-MIC-WIND-250723/4439
N/A	11-Jul-2023	7.3	Volume Shadow Copy Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32054	ability/CVE-2023-32054	
N/A	11-Jul-2023	7.2	Microsoft Failover Cluster Remote Code Execution Vulnerability **CVE ID : CVE-2023-32033**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32033	O-MIC-WIND-250723/4441
N/A	11-Jul-2023	7.2	Windows Active Directory Certificate Services (AD CS) Remote Code Execution Vulnerability **CVE ID : CVE-2023-35350**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35350	O-MIC-WIND-250723/4442
N/A	11-Jul-2023	6.8	Windows Remote Desktop Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32043	O-MIC-WIND-250723/4443
N/A	11-Jul-2023	6.8	Windows Remote Desktop Protocol Security Feature Bypass **CVE ID : CVE-2023-35332**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35332	O-MIC-WIND-250723/4444
N/A	11-Jul-2023	6.7	Active Template Library Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32055	O-MIC-WIND-250723/4445
Concurrent Execution using Shared Resource with	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35310**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35310	O-MIC-WIND-250723/4446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')					
N/A	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35344**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35344	O-MIC-WIND-250723/4447
N/A	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35345**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35345	O-MIC-WIND-250723/4448
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35346**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35346	O-MIC-WIND-250723/4449
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35314	O-MIC-WIND-250723/4450
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Information Disclosure Vulnerability **CVE ID : CVE-2023-35316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35316	O-MIC-WIND-250723/4451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35318**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35318	O-MIC-WIND-250723/4452
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35319**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35319	O-MIC-WIND-250723/4453
N/A	11-Jul-2023	6.5	Windows Deployment Services Denial of Service Vulnerability **CVE ID : CVE-2023-35321**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35321	O-MIC-WIND-250723/4454
N/A	11-Jul-2023	6.5	Windows Authentication Denial of Service Vulnerability **CVE ID : CVE-2023-35329**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35329	O-MIC-WIND-250723/4455
N/A	11-Jul-2023	6.5	Windows Local Security Authority (LSA) Denial of Service Vulnerability **CVE ID : CVE-2023-35331**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35331	O-MIC-WIND-250723/4456
N/A	11-Jul-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35296**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35296	O-MIC-WIND-250723/4457
N/A	11-Jul-2023	6.5	Windows MSHTML Platform Security	https://msrc.microsoft.co	O-MIC-WIND-250723/4458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Feature Bypass Vulnerability **CVE ID : CVE-2023-35308**	m/update-guide/vulnerability/CVE-2023-35308	
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-33164**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33164	O-MIC-WIND-250723/4459
N/A	11-Jul-2023	6.5	Active Directory Federation Service Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35348**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35348	O-MIC-WIND-250723/4460
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32085**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32085	O-MIC-WIND-250723/4461
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35306**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35306	O-MIC-WIND-250723/4462
N/A	11-Jul-2023	5.5	Windows Update Orchestrator Service Information Disclosure Vulnerability **CVE ID : CVE-2023-32041**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32041	O-MIC-WIND-250723/4463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35324	O-MIC-WIND-250723/4464
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32040**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32040	O-MIC-WIND-250723/4465
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32039**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32039	O-MIC-WIND-250723/4466
N/A	11-Jul-2023	5.5	Microsoft DirectMusic Information Disclosure Vulnerability **CVE ID : CVE-2023-35341**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35341	O-MIC-WIND-250723/4467
N/A	11-Jul-2023	5.4	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35336**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35336	O-MIC-WIND-250723/4468
N/A	11-Jul-2023	4.9	Microsoft Failover Cluster Information	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-32083**	ability/CVE-2023-32083	
Product: windows_server_2019					
Affected Version(s): -					
N/A	11-Jul-2023	9.8	Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32056	O-MIC-WIND-250723/4470
N/A	11-Jul-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-32057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32057	O-MIC-WIND-250723/4471
N/A	11-Jul-2023	9.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33154	O-MIC-WIND-250723/4472
N/A	11-Jul-2023	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35315**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35315	O-MIC-WIND-250723/4473
N/A	11-Jul-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35302	O-MIC-WIND-250723/4474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35302		
N/A	11-Jul-2023	8.8	Windows Deployment Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-35322**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35322	O-MIC-WIND-250723/4475
N/A	11-Jul-2023	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32049	O-MIC-WIND-250723/4476
N/A	11-Jul-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-32038**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32038	O-MIC-WIND-250723/4477
N/A	11-Jul-2023	8.8	USB Audio Class System Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35303**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35303	O-MIC-WIND-250723/4478
N/A	11-Jul-2023	8.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-35300**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35300	O-MIC-WIND-250723/4479
N/A	11-Jul-2023	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32053	O-MIC-WIND-250723/4480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21756**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21756	O-MIC-WIND-250723/4481
N/A	11-Jul-2023	7.8	Microsoft VOLSNAP.SYS Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35312	O-MIC-WIND-250723/4482
N/A	11-Jul-2023	7.8	Windows Online Certificate Status Protocol (OCSP) SnapIn Remote Code Execution Vulnerability **CVE ID : CVE-2023-35313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35313	O-MIC-WIND-250723/4483
N/A	11-Jul-2023	7.8	Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35317**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35317	O-MIC-WIND-250723/4484
N/A	11-Jul-2023	7.8	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35320	O-MIC-WIND-250723/4485
N/A	11-Jul-2023	7.8	Windows Transaction Manager Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35328**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35328	O-MIC-WIND-250723/4486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35305**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35305	O-MIC-WIND-250723/4487
N/A	11-Jul-2023	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33155**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33155	O-MIC-WIND-250723/4488
N/A	11-Jul-2023	7.8	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35342**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35342	O-MIC-WIND-250723/4489
N/A	11-Jul-2023	7.8	Windows Geolocation Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-35343**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35343	O-MIC-WIND-250723/4490
N/A	11-Jul-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35299**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35299	O-MIC-WIND-250723/4491
N/A	11-Jul-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35304**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35304	O-MIC-WIND-250723/4492
N/A	11-Jul-2023	7.8	Windows MSHTML Platform Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-250723/4493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2023-32046**	guide/vulnerability/CVE-2023-32046	
N/A	11-Jul-2023	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35340**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35340	O-MIC-WIND-250723/4494
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32034	O-MIC-WIND-250723/4495
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32035**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32035	O-MIC-WIND-250723/4496
N/A	11-Jul-2023	7.5	OLE Automation Information Disclosure Vulnerability **CVE ID : CVE-2023-32042**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32042	O-MIC-WIND-250723/4497
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32044**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32044	O-MIC-WIND-250723/4498
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32045**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32045	O-MIC-WIND-250723/4499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	7.5	Windows Extended Negotiation Denial of Service Vulnerability **CVE ID : CVE-2023-35330**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35330	O-MIC-WIND-250723/4500
N/A	11-Jul-2023	7.5	Windows Print Spooler Information Disclosure Vulnerability **CVE ID : CVE-2023-35325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35325	O-MIC-WIND-250723/4501
N/A	11-Jul-2023	7.5	HTTP.sys Denial of Service Vulnerability **CVE ID : CVE-2023-32084**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32084	O-MIC-WIND-250723/4502
N/A	11-Jul-2023	7.5	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-35297**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35297	O-MIC-WIND-250723/4503
N/A	11-Jul-2023	7.5	Windows Network Load Balancing Remote Code Execution Vulnerability **CVE ID : CVE-2023-33163**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33163	O-MIC-WIND-250723/4504
Concurrent Execution using Shared Resource with Improper Synchronization	11-Jul-2023	7.5	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35309**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35309	O-MIC-WIND-250723/4505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
N/A	11-Jul-2023	7.5	Windows Peer Name Resolution Protocol Denial of Service Vulnerability **CVE ID : CVE-2023-35338**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35338	O-MIC-WIND-250723/4506
N/A	11-Jul-2023	7.5	Windows CryptoAPI Denial of Service Vulnerability **CVE ID : CVE-2023-35339**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35339	O-MIC-WIND-250723/4507
N/A	11-Jul-2023	7.4	Windows Netlogon Information Disclosure Vulnerability **CVE ID : CVE-2023-21526**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21526	O-MIC-WIND-250723/4508
N/A	11-Jul-2023	7.3	Volume Shadow Copy Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32054	O-MIC-WIND-250723/4509
N/A	11-Jul-2023	7.2	Microsoft Failover Cluster Remote Code Execution Vulnerability **CVE ID : CVE-2023-32033**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32033	O-MIC-WIND-250723/4510
N/A	11-Jul-2023	7.2	Windows Active Directory Certificate Services (AD CS) Remote Code Execution Vulnerability **CVE ID : CVE-2023-35350**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35350	O-MIC-WIND-250723/4511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	6.8	Windows Remote Desktop Protocol Security Feature Bypass **CVE ID : CVE-2023-35332**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35332	O-MIC-WIND-250723/4512
N/A	11-Jul-2023	6.8	Windows Remote Desktop Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32043	O-MIC-WIND-250723/4513
N/A	11-Jul-2023	6.7	Active Template Library Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32055	O-MIC-WIND-250723/4514
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35310**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35310	O-MIC-WIND-250723/4515
N/A	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35344**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35344	O-MIC-WIND-250723/4516
N/A	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35345	O-MIC-WIND-250723/4517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35345		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35346**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35346	O-MIC-WIND-250723/4518
N/A	11-Jul-2023	6.5	Windows Deployment Services Denial of Service Vulnerability **CVE ID : CVE-2023-35321**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35321	O-MIC-WIND-250723/4519
N/A	11-Jul-2023	6.5	Windows Authentication Denial of Service Vulnerability **CVE ID : CVE-2023-35329**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35329	O-MIC-WIND-250723/4520
N/A	11-Jul-2023	6.5	Windows Local Security Authority (LSA) Denial of Service Vulnerability **CVE ID : CVE-2023-35331**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35331	O-MIC-WIND-250723/4521
N/A	11-Jul-2023	6.5	Windows Layer-2 Bridge Network Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32037**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32037	O-MIC-WIND-250723/4522
N/A	11-Jul-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver	https://msrc.microsoft.com/update-	O-MIC-WIND-250723/4523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability **CVE ID : CVE-2023-35296**	guide/vulnerability/CVE-2023-35296	
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Information Disclosure Vulnerability **CVE ID : CVE-2023-35316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35316	O-MIC-WIND-250723/4524
N/A	11-Jul-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35308**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35308	O-MIC-WIND-250723/4525
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35318**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35318	O-MIC-WIND-250723/4526
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35319**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35319	O-MIC-WIND-250723/4527
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-33164**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33164	O-MIC-WIND-250723/4528
N/A	11-Jul-2023	6.5	Active Directory Federation Service Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35348	ability/CVE-2023-35348	
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35314	O-MIC-WIND-250723/4530
N/A	11-Jul-2023	5.5	Windows CDP User Components Information Disclosure Vulnerability **CVE ID : CVE-2023-35326**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35326	O-MIC-WIND-250723/4531
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35306**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35306	O-MIC-WIND-250723/4532
N/A	11-Jul-2023	5.5	Microsoft DirectMusic Information Disclosure Vulnerability **CVE ID : CVE-2023-35341**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35341	O-MIC-WIND-250723/4533
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32085**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32085	O-MIC-WIND-250723/4534
N/A	11-Jul-2023	5.5	Windows Update Orchestrator Service	https://msrc.microsoft.co	O-MIC-WIND-250723/4535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability **CVE ID : CVE-2023-32041**	m/update-guide/vulnerability/CVE-2023-32041	
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32040**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32040	O-MIC-WIND-250723/4536
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35324	O-MIC-WIND-250723/4537
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32039**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32039	O-MIC-WIND-250723/4538
N/A	11-Jul-2023	5.4	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35336**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35336	O-MIC-WIND-250723/4539
N/A	11-Jul-2023	4.9	Microsoft Failover Cluster Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32083	ability/CVE-2023-32083	
Product: windows_server_2022					
Affected Version(s): -					
N/A	11-Jul-2023	9.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33154	O-MIC-WIND-250723/4541
N/A	11-Jul-2023	9.8	Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32056	O-MIC-WIND-250723/4542
N/A	11-Jul-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-32057**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32057	O-MIC-WIND-250723/4543
N/A	11-Jul-2023	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-32038**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32038	O-MIC-WIND-250723/4544
N/A	11-Jul-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35302**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35302	O-MIC-WIND-250723/4545
N/A	11-Jul-2023	8.8	USB Audio Class System Driver Remote Code	https://msrc.microsoft.com/update-	O-MIC-WIND-250723/4546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-35303**	guide/vulnerability/CVE-2023-35303	
N/A	11-Jul-2023	8.8	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-35315**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35315	O-MIC-WIND-250723/4547
N/A	11-Jul-2023	8.8	Windows Deployment Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-35322**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35322	O-MIC-WIND-250723/4548
N/A	11-Jul-2023	8.8	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32049**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32049	O-MIC-WIND-250723/4549
N/A	11-Jul-2023	8.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-35300**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35300	O-MIC-WIND-250723/4550
N/A	11-Jul-2023	7.8	Windows Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21756**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21756	O-MIC-WIND-250723/4551
N/A	11-Jul-2023	7.8	Windows Common Log File System Driver Elevation of	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2023-35299**	ability/CVE-2023-35299	
N/A	11-Jul-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35304**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35304	O-MIC-WIND-250723/4553
N/A	11-Jul-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35305**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35305	O-MIC-WIND-250723/4554
N/A	11-Jul-2023	7.8	Windows OLE Remote Code Execution Vulnerability **CVE ID : CVE-2023-35323**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35323	O-MIC-WIND-250723/4555
N/A	11-Jul-2023	7.8	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35320	O-MIC-WIND-250723/4556
N/A	11-Jul-2023	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35340**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35340	O-MIC-WIND-250723/4557
N/A	11-Jul-2023	7.8	Windows Transaction Manager Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35328	ability/CVE-2023-35328	
N/A	11-Jul-2023	7.8	Windows Image Acquisition Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35342**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35342	O-MIC-WIND-250723/4559
N/A	11-Jul-2023	7.8	Windows Geolocation Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-35343**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35343	O-MIC-WIND-250723/4560
N/A	11-Jul-2023	7.8	Windows MSHTML Platform Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32046**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046	O-MIC-WIND-250723/4561
N/A	11-Jul-2023	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2023-32053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32053	O-MIC-WIND-250723/4562
N/A	11-Jul-2023	7.8	Windows Online Certificate Status Protocol (OCSP) SnapIn Remote Code Execution Vulnerability **CVE ID : CVE-2023-35313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35313	O-MIC-WIND-250723/4563
N/A	11-Jul-2023	7.8	Microsoft VOLSNAP.SYS Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35312	ability/CVE-2023-35312	
N/A	11-Jul-2023	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35337**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35337	O-MIC-WIND-250723/4565
N/A	11-Jul-2023	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33155**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33155	O-MIC-WIND-250723/4566
N/A	11-Jul-2023	7.8	Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35317**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35317	O-MIC-WIND-250723/4567
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32034**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32034	O-MIC-WIND-250723/4568
N/A	11-Jul-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-32035**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32035	O-MIC-WIND-250723/4569
N/A	11-Jul-2023	7.5	OLE Automation Information Disclosure Vulnerability **CVE ID : CVE-2023-32042**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32042	O-MIC-WIND-250723/4570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-32045**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32045	O-MIC-WIND-250723/4571
N/A	11-Jul-2023	7.5	Windows Network Load Balancing Remote Code Execution Vulnerability **CVE ID : CVE-2023-33163**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33163	O-MIC-WIND-250723/4572
N/A	11-Jul-2023	7.5	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-35297**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35297	O-MIC-WIND-250723/4573
N/A	11-Jul-2023	7.5	Windows Print Spooler Information Disclosure Vulnerability **CVE ID : CVE-2023-35325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35325	O-MIC-WIND-250723/4574
N/A	11-Jul-2023	7.5	HTTP.sys Denial of Service Vulnerability **CVE ID : CVE-2023-35298**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35298	O-MIC-WIND-250723/4575
N/A	11-Jul-2023	7.5	Windows Extended Negotiation Denial of Service Vulnerability **CVE ID : CVE-2023-35330**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35330	O-MIC-WIND-250723/4576
N/A	11-Jul-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-250723/4577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32044	guide/vulnerability/CVE-2023-32044	
N/A	11-Jul-2023	7.5	Windows Peer Name Resolution Protocol Denial of Service Vulnerability **CVE ID : CVE-2023-35338**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35338	O-MIC-WIND-250723/4578
N/A	11-Jul-2023	7.5	Windows CryptoAPI Denial of Service Vulnerability **CVE ID : CVE-2023-35339**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35339	O-MIC-WIND-250723/4579
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	7.5	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35309**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35309	O-MIC-WIND-250723/4580
N/A	11-Jul-2023	7.5	HTTP.sys Denial of Service Vulnerability **CVE ID : CVE-2023-32084**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32084	O-MIC-WIND-250723/4581
N/A	11-Jul-2023	7.4	Windows Netlogon Information Disclosure Vulnerability **CVE ID : CVE-2023-21526**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21526	O-MIC-WIND-250723/4582
N/A	11-Jul-2023	7.3	Volume Shadow Copy Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-250723/4583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2023-32054**	guide/vulnerability/CVE-2023-32054	
N/A	11-Jul-2023	7.2	Microsoft Failover Cluster Remote Code Execution Vulnerability **CVE ID : CVE-2023-32033**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32033	O-MIC-WIND-250723/4584
N/A	11-Jul-2023	7.2	Windows Active Directory Certificate Services (AD CS) Remote Code Execution Vulnerability **CVE ID : CVE-2023-35350**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35350	O-MIC-WIND-250723/4585
N/A	11-Jul-2023	7.1	Microsoft Install Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35347**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35347	O-MIC-WIND-250723/4586
N/A	11-Jul-2023	6.8	Windows Remote Desktop Security Feature Bypass Vulnerability **CVE ID : CVE-2023-32043**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32043	O-MIC-WIND-250723/4587
N/A	11-Jul-2023	6.8	Windows Remote Desktop Protocol Security Feature Bypass **CVE ID : CVE-2023-35332**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35332	O-MIC-WIND-250723/4588
N/A	11-Jul-2023	6.7	Active Template Library Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32055	ability/CVE-2023-32055	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35310**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35310	O-MIC-WIND-250723/4590
N/A	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35344**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35344	O-MIC-WIND-250723/4591
N/A	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35345**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35345	O-MIC-WIND-250723/4592
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Jul-2023	6.6	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35346**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35346	O-MIC-WIND-250723/4593
N/A	11-Jul-2023	6.5	Windows Deployment Services Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-250723/4594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35321	ability/CVE-2023-35321	
N/A	11-Jul-2023	6.5	Windows Layer-2 Bridge Network Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32037**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32037	O-MIC-WIND-250723/4595
N/A	11-Jul-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35308**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35308	O-MIC-WIND-250723/4596
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-33164**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33164	O-MIC-WIND-250723/4597
N/A	11-Jul-2023	6.5	Windows Authentication Denial of Service Vulnerability **CVE ID : CVE-2023-35329**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35329	O-MIC-WIND-250723/4598
N/A	11-Jul-2023	6.5	Windows Local Security Authority (LSA) Denial of Service Vulnerability **CVE ID : CVE-2023-35331**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35331	O-MIC-WIND-250723/4599
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35314	O-MIC-WIND-250723/4600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35296**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35296	O-MIC-WIND-250723/4601
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Information Disclosure Vulnerability **CVE ID : CVE-2023-35316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35316	O-MIC-WIND-250723/4602
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35318**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35318	O-MIC-WIND-250723/4603
N/A	11-Jul-2023	6.5	Active Directory Federation Service Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35348**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35348	O-MIC-WIND-250723/4604
N/A	11-Jul-2023	6.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-35319**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35319	O-MIC-WIND-250723/4605
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32040	O-MIC-WIND-250723/4606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32040		
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32039**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32039	O-MIC-WIND-250723/4607
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35324	O-MIC-WIND-250723/4608
N/A	11-Jul-2023	5.5	Windows CDP User Components Information Disclosure Vulnerability **CVE ID : CVE-2023-35326**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35326	O-MIC-WIND-250723/4609
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-32085**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32085	O-MIC-WIND-250723/4610
N/A	11-Jul-2023	5.5	Windows Update Orchestrator Service Information Disclosure Vulnerability **CVE ID : CVE-2023-32041**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32041	O-MIC-WIND-250723/4611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Jul-2023	5.5	Microsoft DirectMusic Information Disclosure Vulnerability **CVE ID : CVE-2023-35341**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35341	O-MIC-WIND-250723/4612
N/A	11-Jul-2023	5.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-35306**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35306	O-MIC-WIND-250723/4613
N/A	11-Jul-2023	5.4	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35336**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35336	O-MIC-WIND-250723/4614
N/A	11-Jul-2023	4.9	Microsoft Failover Cluster Information Disclosure Vulnerability **CVE ID : CVE-2023-32083**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32083	O-MIC-WIND-250723/4615
Vendor: milesight					
Product: ur-32l_firmware					
Affected Version(s): 32.3.0.5					
Stack-based Buffer Overflow	06-Jul-2023	9.8	A stack-based buffer overflow vulnerability exists in the libzebra.so.0.0.0 security_decrypt_password functionality of Milesight UR32L v32.3.0.5. A specially crafted HTTP	N/A	O-MIL-UR-3-250723/4616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request can lead to a buffer overflow. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2023-24018**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_qos function with the attach_class variable. **CVE ID : CVE-2023-25097**	N/A	O-MIL-UR-3-250723/4617
Product: ur32l_firmware					
Affected Version(s): 32.3.0.5					
Stack-based Buffer Overflow	06-Jul-2023	9.8	A buffer overflow vulnerability exists in the uhttpd login functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to remote code execution. An	N/A	O-MIL-UR32-250723/4618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2023-23902**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jul-2023	9.8	An OS command injection vulnerability exists in the vtysh_ubus tcpdump_start_cb functionality of Milesight UR32L v32.3.0.5. A specially crafted HTTP request can lead to command execution. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2023-22653**	N/A	O-MIL-UR32-250723/4619
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jul-2023	8.8	An OS command injection vulnerability exists in the vtysh_ubus _get_fw_logs functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to command execution. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2023-22299**	N/A	O-MIL-UR32-250723/4620
Improper Neutralizat	06-Jul-2023	8.8	Two OS command injection	N/A	O-MIL-UR32-250723/4621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			vulnerability exist in the vtysh_ubus toolsh_excute.constprop.1 functionality of Milesight UR32L v32.3.0.5. A specially-crafted network request can lead to command execution. An attacker can send a network request to trigger these vulnerabilities.This command injection is in the ping tool utility. **CVE ID : CVE-2023-24519**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jul-2023	8.8	Two OS command injection vulnerability exist in the vtysh_ubus toolsh_excute.constprop.1 functionality of Milesight UR32L v32.3.0.5. A specially-crafted network request can lead to command execution. An attacker can send a network request to trigger these vulnerabilities.This command injection is in the trace tool utility. **CVE ID : CVE-2023-24520**	N/A	O-MIL-UR32-250723/4622
Improper Neutralization of	06-Jul-2023	8.8	Two OS command injection vulnerabilities exist	N/A	O-MIL-UR32-250723/4623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			in the urvpn_client cmd_name_action functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to arbitrary command execution. An attacker can send a network request to trigger these vulnerabilities.This OS command injection is triggered through a UDP packet. **CVE ID : CVE-2023-24583**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jul-2023	8.8	Two OS command injection vulnerabilities exist in the urvpn_client cmd_name_action functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to arbitrary command execution. An attacker can send a network request to trigger these vulnerabilities.This OS command injection is triggered through a TCP packet. **CVE ID : CVE-2023-24582**	N/A	O-MIL-UR32-250723/4624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2023	8.1	A stack-based buffer overflow vulnerability exists in the urvpn_client http_connection_readcb functionality of Milesight UR32L v32.3.0.5. A specially crafted network packet can lead to a buffer overflow. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2023-24019**	N/A	O-MIL-UR32-250723/4625
Improper Certificate Validation	06-Jul-2023	8.1	A misconfiguration vulnerability exists in the urvpn_client functionality of Milesight UR32L v32.3.0.5. A specially-crafted man-in-the-middle attack can lead to increased privileges. An attacker can perform a man-in-the-middle attack to trigger this vulnerability. **CVE ID : CVE-2023-23546**	N/A	O-MIL-UR32-250723/4626
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially	N/A	O-MIL-UR32-250723/4627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_pptp function with the remote_subnet and the remote_mask variables. **CVE ID : CVE-2023-25119**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_dmvpn function with the cisco_secret variable. **CVE ID : CVE-2023-25120**	N/A	O-MIL-UR32-250723/4628
Stack-based	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus	N/A	O-MIL-UR32-250723/4629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_ike_profile function with the secrets_local variable. **CVE ID : CVE-2023-25121**		
Out-of-bounds Write	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the old_remote_subnet and the	N/A	O-MIL-UR32-250723/4630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			old_remote_mask variables. **CVE ID : CVE-2023-25122**		
Buffer Over-read	06-Jul-2023	7.5	An access violation vulnerability exists in the eventcore functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to denial of service. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2023-23571**	N/A	O-MIL-UR32-250723/4631
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the remote_subnet and the remote_mask	N/A	O-MIL-UR32-250723/4632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variables when action is 2. **CVE ID : CVE-2023-25123**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the remote_subnet and the remote_mask variables. **CVE ID : CVE-2023-25124**	N/A	O-MIL-UR32-250723/4633
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to	N/A	O-MIL-UR32-250723/4634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the src and dmz variables. **CVE ID : CVE-2023-25081**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the old_ip and old_mac variables. **CVE ID : CVE-2023-25082**	N/A	O-MIL-UR32-250723/4635
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP	N/A	O-MIL-UR32-250723/4636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the ip and mac variables. **CVE ID : CVE-2023-25083**		
Out-of-bounds Write	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the ip, mac and description variables. **CVE ID : CVE-2023-25084**	N/A	O-MIL-UR32-250723/4637
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due	N/A	O-MIL-UR32-250723/4638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the index and to_dst variables. **CVE ID : CVE-2023-25085**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the index and dport variables. **CVE ID : CVE-2023-25086**	N/A	O-MIL-UR32-250723/4639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the index and to_dport variables. **CVE ID : CVE-2023-25087**	N/A	O-MIL-UR32-250723/4640
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set	N/A	O-MIL-UR32-250723/4641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function with the index and description variables. **CVE ID : CVE-2023-25088**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the handle_interface_acl function with the interface variable when in_acl is -1. **CVE ID : CVE-2023-25089**	N/A	O-MIL-UR32-250723/4642
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send	N/A	O-MIL-UR32-250723/4643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the handle_interface_acl function with the interface and in_acl variables. **CVE ID : CVE-2023-25090**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the handle_interface_acl function with the interface variable when out_acl is -1. **CVE ID : CVE-2023-25091**	N/A	O-MIL-UR32-250723/4644
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf	N/A	O-MIL-UR32-250723/4645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the handle_interface_acl function with the interface and out_acl variables. **CVE ID : CVE-2023-25092**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_qos function with the class_name variable.. **CVE ID : CVE-2023-25093**	N/A	O-MIL-UR32-250723/4646
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight	N/A	O-MIL-UR32-250723/4647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the into_class_node function with either the class_name or old_class_name variable. **CVE ID : CVE-2023-25094**		
Out-of-bounds Write	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_qos function with the rule_name variable with two possible format strings that	N/A	O-MIL-UR32-250723/4648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			represent negated commands. **CVE ID : CVE-2023-25095**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_qos function with the rule_name variable with two possible format strings. **CVE ID : CVE-2023-25096**	N/A	O-MIL-UR32-250723/4649
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these	N/A	O-MIL-UR32-250723/4650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities.This buffer overflow occurs in the set_qos function with the source variable. **CVE ID : CVE-2023-25098**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_qos function with the dest variable. **CVE ID : CVE-2023-25099**	N/A	O-MIL-UR32-250723/4651
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to	N/A	O-MIL-UR32-250723/4652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trigger these vulnerabilities.This buffer overflow occurs in the set_qos function with the default_class variable. **CVE ID : CVE-2023-25100**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_dmvpn function with the gre_key variable. **CVE ID : CVE-2023-25101**	N/A	O-MIL-UR32-250723/4653
Out-of-bounds Write	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a	N/A	O-MIL-UR32-250723/4654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_dmvpn function with the hub_ip and the hub_gre_ip variables. **CVE ID : CVE-2023-25102**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_dmvpn function with the gre_ip and the gre_mask variables. **CVE ID : CVE-2023-25103**	N/A	O-MIL-UR32-250723/4655
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due	N/A	O-MIL-UR32-250723/4656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_ike_profile function with the username and the password variables. **CVE ID : CVE-2023-25104**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_ike_profile function with the secrets_remote variable. **CVE ID : CVE-2023-25105**	N/A	O-MIL-UR32-250723/4657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_gre function with the local_virtual_ip and the local_virtual_mask variables. **CVE ID : CVE-2023-25106**	N/A	O-MIL-UR32-250723/4658
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_gre	N/A	O-MIL-UR32-250723/4659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function with the remote_subnet and the remote_mask variables. **CVE ID : CVE-2023-25107**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_gre function with the remote_ip variable. **CVE ID : CVE-2023-25108**	N/A	O-MIL-UR32-250723/4660
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these	N/A	O-MIL-UR32-250723/4661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities.This buffer overflow occurs in the set_gre function with the local_ip variable. **CVE ID : CVE-2023-25109**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_gre function with the remote_virtual_ip variable. **CVE ID : CVE-2023-25110**	N/A	O-MIL-UR32-250723/4662
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send	N/A	O-MIL-UR32-250723/4663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_gre function with the key variable. **CVE ID : CVE-2023-25111**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_l2tp function with the remote_subnet and the remote_mask variables. **CVE ID : CVE-2023-25112**	N/A	O-MIL-UR32-250723/4664
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP	N/A	O-MIL-UR32-250723/4665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_l2tp function with the key variable. **CVE ID : CVE-2023-25113**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the expert_options variable. **CVE ID : CVE-2023-25114**	N/A	O-MIL-UR32-250723/4666
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an	N/A	O-MIL-UR32-250723/4667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the remote_ip and the port variables. **CVE ID : CVE-2023-25115**		
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the local_virtual_ip and the remote_virtual_ip variables. **CVE ID : CVE-2023-25116**	N/A	O-MIL-UR32-250723/4668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the local_virtual_ip and the local_virtual_mask variables. **CVE ID : CVE-2023-25117**	N/A	O-MIL-UR32-250723/4669
Stack-based Buffer Overflow	06-Jul-2023	7.5	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to a buffer overflow. An attacker can send HTTP requests to trigger these vulnerabilities.This buffer overflow	N/A	O-MIL-UR32-250723/4670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			occurs in the set_openvpn_client function with the username and the password variables. **CVE ID : CVE-2023-25118**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jul-2023	7.2	An OS command injection vulnerability exists in the libzebra.so bridge_group functionality of Milesight UR32L v32.3.0.5. A specially crafted network packet can lead to command execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2023-22306**	N/A	O-MIL-UR32-250723/4671
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jul-2023	7.2	An OS command injection vulnerability exists in the ys_thirdparty check_system_user functionality of Milesight UR32L v32.3.0.5. A specially crafted set of network packets can lead to command execution. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2023-22365**	N/A	O-MIL-UR32-250723/4672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jul-2023	7.2	An os command injection vulnerability exists in the libzebra.so change_hostname functionality of Milesight UR32L v32.3.0.5. A specially-crafted network packets can lead to command execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2023-22659**	N/A	O-MIL-UR32-250723/4673
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jul-2023	7.2	An OS command injection vulnerability exists in the ys_thirdparty user_delete functionality of Milesight UR32L v32.3.0.5. A specially crafted network packet can lead to command execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2023-23550**	N/A	O-MIL-UR32-250723/4674
Improper Neutralization of Special Elements used in an OS Command	06-Jul-2023	7.2	An OS command injection vulnerability exists in the ys_thirdparty system_user_script functionality of Milesight UR32L v32.3.0.5. A specially	N/A	O-MIL-UR32-250723/4675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			crafted series of network requests can lead to command execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2023-24595**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jul-2023	7.2	Two OS command injection vulnerabilities exist in the zebra vlan_name functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to command execution. An attacker can send a network request to trigger these vulnerabilities.This command injection is in the code branch that manages an already existing vlan configuration. **CVE ID : CVE-2023-25582**	N/A	O-MIL-UR32-250723/4676
Improper Neutralization of Special Elements used in an OS Command ('OS	06-Jul-2023	7.2	Two OS command injection vulnerabilities exist in the zebra vlan_name functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to command execution.	N/A	O-MIL-UR32-250723/4677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			An attacker can send a network request to trigger these vulnerabilities.This command injection is in the code branch that manages a new vlan configuration. **CVE ID : CVE-2023-25583**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jul-2023	6.5	A directory traversal vulnerability exists in the luci2-io file-export mib functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to arbitrary file read. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2023-23547**	N/A	O-MIL-UR32-250723/4678
Vendor: Moxa					
Product: tn-5900_firmware					
Affected Version(s): * Up to (including) 3.3					
Observable Discrepancy	05-Jul-2023	5.3	TN-5900 Series version 3.3 and prior versions is vulnearble to user enumeration vulnerability. The vulnerability may allow a remote attacker to determine whether a user is valid during password recovery through the web	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-230401-tn-5900-series-user-enumeration	O-MOX-TN-5-250723/4679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			login page and enable a brute force attack with valid users. **CVE ID : CVE-2023-3336**	- vulnerability	
Vendor: nio					
Product: aspen					
Affected Version(s): * Up to (excluding) 3.3.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jul-2023	7.8	An issue in the com.nextev.datastatistic component of NIO EC6 Aspen before v3.3.0 allows attackers to escalate privileges via path traversal. **CVE ID : CVE-2023-24256**	N/A	O-NIO-ASPE-250723/4680
Vendor: Nvidia					
Product: dgx_a100_firmware					
Affected Version(s): * Up to (excluding) 1.21					
Improper Privilege Management	04-Jul-2023	7.8	NVIDIA DGX A100/A800 contains a vulnerability in SBIOS where an attacker may cause execution with unnecessary privileges by leveraging a	https://nvidia.custhelp.com/app/answers/detail/a_id/5461	O-NVI-DGX_-250723/4681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			weakness whereby proper input parameter validation is not performed. A successful exploit of this vulnerability may lead to denial of service, information disclosure, and data tampering. **CVE ID : CVE-2023-25521**		
Improper Input Validation	04-Jul-2023	7.8	NVIDIA DGX A100/A800 contains a vulnerability in SBIOS where an attacker may cause improper input validation by providing configuration information in an unexpected format. A successful exploit of this vulnerability may lead to denial of	https://nvidia.custhelp.com/app/answers/detail/a_id/5461	O-NVI-DGX_-250723/4682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, information disclosure, and data tampering. **CVE ID : CVE-2023-25522**		
Product: dgx_a800_firmware					
Affected Version(s): * Up to (excluding) 1.21					
Improper Privilege Management	04-Jul-2023	7.8	NVIDIA DGX A100/A800 contains a vulnerability in SBIOS where an attacker may cause execution with unnecessary privileges by leveraging a weakness whereby proper input parameter validation is not performed. A successful exploit of this vulnerability may lead to denial of service, information	https://nvidia.custhelp.com/app/answers/detail/a_id/5461	O-NVI-DGX_-250723/4683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure, and data tampering. **CVE ID : CVE-2023-25521**		
Improper Input Validation	04-Jul-2023	7.8	NVIDIA DGX A100/A800 contains a vulnerability in SBIOS where an attacker may cause improper input validation by providing configuration information in an unexpected format. A successful exploit of this vulnerability may lead to denial of service, information disclosure, and data tampering.	https://nvidia.custhelp.com/app/answers/detail/a_id/5461	O-NVI-DGX_-250723/4684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25522		
Vendor: openwrt					
Product: openwrt					
Affected Version(s): 21.02					
Out-of-bounds Write	04-Jul-2023	6.7	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07978760; Issue ID: ALPS07363410. **CVE ID : CVE-2023-20775**	https://corp.mediatek.com/product-security-bulletin/July-2023	O-OPE-OPEN-250723/4685
Vendor: Oracle					
Product: solaris					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code via	https://exchange.xforce.ibmcloud.com/vulnerabilities/249514, https://www.ibm.com/s	O-ORA-SOLA-250723/4686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JNDI Injection. By sending a specially crafted request using the property clientRerouteServer ListJNDIName, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249514. **CVE ID : CVE-2023-27867**	upport/pages/node/7010029	
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked class instantiation when providing plugin classes. By sending a specially crafted request using the named pluginClassName class, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249516. **CVE ID : CVE-2023-27868**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249516, https://www.ibm.com/support/pages/node/7010029	O-ORA-SOLA-250723/4687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	10-Jul-2023	8.8	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked logger injection. By sending a specially crafted request using the named traceFile property, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249517. **CVE ID : CVE-2023-27869**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249517, https://www.ibm.com/support/pages/node/7010029	O-ORA-SOLA-250723/4688
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Jul-2023	7.8	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 db2set is vulnerable to a buffer overflow, caused by improper bounds checking. An attacker could overflow the buffer and execute arbitrary code. IBM X-Force ID: 252184. **CVE ID : CVE-2023-30431**	https://www.ibm.com/support/pages/node/7010565, https://exchange.xforce.ibmcloud.com/vulnerabilities/252184	O-ORA-SOLA-250723/4689
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1	https://www.ibm.com/support/pages/node/701	O-ORA-SOLA-250723/4690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 11.5 federated server is vulnerable to a denial of service as the server may crash when using a specially crafted wrapper using certain options. IBM X-Force ID: 253202. **CVE ID : CVE-2023-30442**	0561, https://exchange.xforce.ibmcloud.com/vulnerabilities/253202	
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253357. **CVE ID : CVE-2023-30445**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253357, https://www.ibm.com/support/pages/node/7010557	O-ORA-SOLA-250723/4691
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253361 .	https://www.ibm.com/support/pages/node/7010557, https://exchange.xforce.ibmcloud.com/vulnerabilities/253361	O-ORA-SOLA-250723/4692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30446		
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253436. **CVE ID : CVE-2023-30447**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253436, https://www.ibm.com/support/pages/node/7010557	O-ORA-SOLA-250723/4693
N/A	10-Jul-2023	7.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253437. **CVE ID : CVE-2023-30448**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253437, https://www.ibm.com/support/pages/node/7010557	O-ORA-SOLA-250723/4694
N/A	10-Jul-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query. IBM X-Force ID: 253439.	https://exchange.xforce.ibmcloud.com/vulnerabilities/253439, https://www.ibm.com/support/pages/node/7010557	O-ORA-SOLA-250723/4695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30449		
Improper Privilege Management	10-Jul-2023	6.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to an information disclosure due to improper privilege management when certain federation features are used. IBM X-Force ID: 252046. **CVE ID : CVE-2023-29256**	https://www.ibm.com/support/pages/node/7010573, https://exchange.xforce.ibmcloud.com/vulnerabilities/252046	O-ORA-SOLA-250723/4696
N/A	10-Jul-2023	4.3	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is vulnerable to insufficient audit logging. IBM X-Force ID: 245918. **CVE ID : CVE-2023-23487**	https://exchange.xforce.ibmcloud.com/vulnerabilities/245918, https://www.ibm.com/support/pages/node/7010567	O-ORA-SOLA-250723/4697
Vendor: ovarro					
Product: tbox_lt2_firmware					
Affected Version(s): -					
Cleartext Storage of Sensitive Information	03-Jul-2023	6.5	?All versions of the TWinSoft Configuration Tool store encrypted passwords as plaintext in memory. An attacker with access to system files	N/A	O-OVA-TBOX-250723/4698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could open a file to load the document into memory, including sensitive information associated with document, such as password. The attacker could then obtain the plaintext password by using a memory viewer. **CVE ID : CVE-2023-3395**		
Affected Version(s): * Up to (including) 1.50.598					
Inclusion of Functionality from Untrusted Control Sphere	03-Jul-2023	7.2	The affected TBox RTUs run OpenVPN with root privileges and can run user defined configuration scripts. An attacker could set up a local OpenVPN server and push a malicious script onto the TBox host to acquire root privileges. **CVE ID : CVE-2023-36609**	N/A	O-OVA-TBOX-250723/4699
Improper Authorization	03-Jul-2023	6.5	The affected TBox RTUs allow low privilege users to access software	N/A	O-OVA-TBOX-250723/4700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security tokens of higher privilege. This could allow an attacker with “user” privileges to access files requiring higher privileges by establishing an SSH session and providing the other tokens. **CVE ID : CVE-2023-36611**		
Insufficient Entropy	03-Jul-2023	5.9	?The affected TBox RTUs generate software security tokens using insufficient entropy. The random seed used to generate the software tokens is not initialized correctly, and other parts of the token are generated using predictable time-based values. An attacker with this knowledge could successfully brute force the token and authenticate themselves. **CVE ID : CVE-2023-36610**	N/A	O-OVA-TBOX-250723/4701
Affected Version(s): From (including) 1.46 Up to (including) 1.50.598					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of a Broken or Risky Cryptographic Algorithm	03-Jul-2023	6.5	The affected TBox RTUs store hashed passwords using MD5 encryption, which is an insecure encryption algorithm. **CVE ID : CVE-2023-36608**	N/A	O-OVA-TBOX-250723/4702
Product: tbox_ms-cpu32-s2_firmware					
Affected Version(s): -					
Cleartext Storage of Sensitive Information	03-Jul-2023	6.5	?All versions of the TWinSoft Configuration Tool store encrypted passwords as plaintext in memory. An attacker with access to system files could open a file to load the document into memory, including sensitive information associated with document, such as password. The attacker could then obtain the plaintext password by using a memory viewer. **CVE ID : CVE-2023-3395**	N/A	O-OVA-TBOX-250723/4703
Affected Version(s): * Up to (including) 1.50.598					
Inclusion of	03-Jul-2023	7.2		N/A	O-OVA-TBOX-250723/4704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Functionality from Untrusted Control Sphere			The affected TBox RTUs run OpenVPN with root privileges and can run user defined configuration scripts. An attacker could set up a local OpenVPN server and push a malicious script onto the TBox host to acquire root privileges. **CVE ID : CVE-2023-36609**		
Improper Authorization	03-Jul-2023	6.5	The affected TBox RTUs allow low privilege users to access software security tokens of higher privilege. This could allow an attacker with "user" privileges to access files requiring higher privileges by establishing an SSH session and providing the other tokens. **CVE ID : CVE-2023-36611**	N/A	O-OVA-TBOX-250723/4705
Insufficient Entropy	03-Jul-2023	5.9	?The affected TBox RTUs generate software security	N/A	O-OVA-TBOX-250723/4706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tokens using insufficient entropy. The random seed used to generate the software tokens is not initialized correctly, and other parts of the token are generated using predictable time-based values. An attacker with this knowledge could successfully brute force the token and authenticate themselves. **CVE ID : CVE-2023-36610**		
Affected Version(s): From (including) 1.46 Up to (including) 1.50.598					
Use of a Broken or Risky Cryptographic Algorithm	03-Jul-2023	6.5	The affected TBox RTUs store hashed passwords using MD5 encryption, which is an insecure encryption algorithm. **CVE ID : CVE-2023-36608**	N/A	O-OVA-TBOX-250723/4707
Product: tbox_ms-cpu32_firmware					
Affected Version(s): -					
Cleartext Storage of Sensitive Information	03-Jul-2023	6.5	?All versions of the TWinSoft Configuration Tool store encrypted passwords as	N/A	O-OVA-TBOX-250723/4708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			plaintext in memory. An attacker with access to system files could open a file to load the document into memory, including sensitive information associated with document, such as password. The attacker could then obtain the plaintext password by using a memory viewer. **CVE ID : CVE-2023-3395**		
Affected Version(s): * Up to (including) 1.50.598					
Inclusion of Functionality from Untrusted Control Sphere	03-Jul-2023	7.2	The affected TBox RTUs run OpenVPN with root privileges and can run user defined configuration scripts. An attacker could set up a local OpenVPN server and push a malicious script onto the TBox host to acquire root privileges. **CVE ID : CVE-2023-36609**	N/A	O-OVA-TBOX-250723/4709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authorization	03-Jul-2023	6.5	The affected TBox RTUs allow low privilege users to access software security tokens of higher privilege. This could allow an attacker with "user" privileges to access files requiring higher privileges by establishing an SSH session and providing the other tokens. **CVE ID : CVE-2023-36611**	N/A	O-OVA-TBOX-250723/4710
Insufficient Entropy	03-Jul-2023	5.9	?The affected TBox RTUs generate software security tokens using insufficient entropy. The random seed used to generate the software tokens is not initialized correctly, and other parts of the token are generated using predictable time-based values. An attacker with this knowledge could successfully brute force the token and authenticate themselves.	N/A	O-OVA-TBOX-250723/4711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36610		
Affected Version(s): From (including) 1.46 Up to (including) 1.50.598					
Use of a Broken or Risky Cryptographic Algorithm	03-Jul-2023	6.5	The affected TBox RTUs store hashed passwords using MD5 encryption, which is an insecure encryption algorithm. **CVE ID : CVE-2023-36608**	N/A	O-OVA-TBOX-250723/4712
Product: tbox_rm2_firmware					
Affected Version(s): -					
Cleartext Storage of Sensitive Information	03-Jul-2023	6.5	?All versions of the TWinSoft Configuration Tool store encrypted passwords as plaintext in memory. An attacker with access to system files could open a file to load the document into memory, including sensitive information associated with document, such as password. The attacker could then obtain the plaintext password by using a memory viewer.	N/A	O-OVA-TBOX-250723/4713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3395		
Affected Version(s): * Up to (including) 1.50.598					
Inclusion of Functionality from Untrusted Control Sphere	03-Jul-2023	7.2	The affected TBox RTUs run OpenVPN with root privileges and can run user defined configuration scripts. An attacker could set up a local OpenVPN server and push a malicious script onto the TBox host to acquire root privileges. **CVE ID : CVE-2023-36609**	N/A	O-OVA-TBOX-250723/4714
Improper Authorization	03-Jul-2023	6.5	The affected TBox RTUs allow low privilege users to access software security tokens of higher privilege. This could allow an attacker with “user” privileges to access files requiring higher privileges by establishing an SSH session and providing the other tokens.	N/A	O-OVA-TBOX-250723/4715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36611		
Insufficient Entropy	03-Jul-2023	5.9	?The affected TBox RTUs generate software security tokens using insufficient entropy. The random seed used to generate the software tokens is not initialized correctly, and other parts of the token are generated using predictable time-based values. An attacker with this knowledge could successfully brute force the token and authenticate themselves. **CVE ID : CVE-2023-36610**	N/A	O-OVA-TBOX-250723/4716
Affected Version(s): From (including) 1.46 Up to (including) 1.50.598					
Use of a Broken or Risky Cryptographic Algorithm	03-Jul-2023	6.5	The affected TBox RTUs store hashed passwords using MD5 encryption, which is an insecure encryption algorithm. **CVE ID : CVE-2023-36608**	N/A	O-OVA-TBOX-250723/4717
Product: tbox_tg2_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Storage of Sensitive Information	03-Jul-2023	6.5	?All versions of the TWinSoft Configuration Tool store encrypted passwords as plaintext in memory. An attacker with access to system files could open a file to load the document into memory, including sensitive information associated with document, such as password. The attacker could then obtain the plaintext password by using a memory viewer. **CVE ID : CVE-2023-3395**	N/A	O-OVA-TBOX-250723/4718
Affected Version(s): * Up to (including) 1.50.598					
Inclusion of Functionality from Untrusted Control Sphere	03-Jul-2023	7.2	The affected TBox RTUs run OpenVPN with root privileges and can run user defined configuration scripts. An attacker could set up a local OpenVPN server and push a malicious script onto the TBox host to acquire root privileges.	N/A	O-OVA-TBOX-250723/4719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36609		
Improper Authorization	03-Jul-2023	6.5	The affected TBox RTUs allow low privilege users to access software security tokens of higher privilege. This could allow an attacker with "user" privileges to access files requiring higher privileges by establishing an SSH session and providing the other tokens. **CVE ID : CVE-2023-36611**	N/A	O-OVA-TBOX-250723/4720
Insufficient Entropy	03-Jul-2023	5.9	?The affected TBox RTUs generate software security tokens using insufficient entropy. The random seed used to generate the software tokens is not initialized correctly, and other parts of the token are generated using predictable time-based values. An attacker with this knowledge could successfully brute	N/A	O-OVA-TBOX-250723/4721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			force the token and authenticate themselves. **CVE ID : CVE-2023-36610**		
Affected Version(s): From (including) 1.46 Up to (including) 1.50.598					
Use of a Broken or Risky Cryptographic Algorithm	03-Jul-2023	6.5	The affected TBox RTUs store hashed passwords using MD5 encryption, which is an insecure encryption algorithm. **CVE ID : CVE-2023-36608**	N/A	O-OVA-TBOX-250723/4722
Vendor: paxtechnology					
Product: pax_a930_firmware					
Affected Version(s): paydroid_7.1.1_virgo_v04.5.02_20220722					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Jul-2023	6.8	PAX A930 device with PayDroid_7.1.1_Virgo_V04.5.02_20220722 can allow the execution of arbitrary commands by using the exec service and including a specific word in the command to be executed. The attacker must have physical USB access to the device in order to exploit this vulnerability. **CVE ID : CVE-2023-27198**	N/A	O-PAX-PAX_-250723/4723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Jul-2023	6.7	PAX A930 device with PayDroid_7.1.1_Virgo_V04.5.02_20220722 can allow an attacker to gain root access by running a crafted binary leveraging an exported function from a shared library. The attacker must have shell access to the device in order to exploit this vulnerability. **CVE ID : CVE-2023-27197**	N/A	O-PAX-PAX_-250723/4724
N/A	05-Jul-2023	6.7	PAX Technology A930 PayDroid_7.1.1_Virgo_V04.5.02_20220722 allows attackers to compile a malicious shared library and use LD_PRELOAD to bypass authorization checks. **CVE ID : CVE-2023-27199**	N/A	O-PAX-PAX_-250723/4725
Vendor: piigab					
Product: m-bus_900s_firmware					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	06-Jul-2023	9.8	The number of login attempts is not limited. This could allow an attacker to perform a brute	N/A	O-PII-M-BU-250723/4726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			force on HTTP basic authentication. **CVE ID : CVE-2023-33868**		
Use of Password Hash With Insufficient Computational Effort	07-Jul-2023	9.8	PiiGAB M-Bus stores passwords using a weak hash algorithm. **CVE ID : CVE-2023-34433**	N/A	O-PII-M-BU-250723/4727
Weak Password Requirements	07-Jul-2023	9.8		N/A	O-PII-M-BU-250723/4728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			There are no requirements for setting a complex password for PiiGAB M-Bus, which could contribute to a successful brute force attack if the password is inline with recommended password guidelines. **CVE ID : CVE-2023-34995**		
Use of Hard-coded Credentials	06-Jul-2023	9.8	PiiGAB M-Bus contains hard-coded credentials which it	N/A	O-PII-M-BU-250723/4729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uses for authentication. **CVE ID : CVE-2023-35987**		
Improper Control of Generation of Code ('Code Injection')	06-Jul-2023	9.8	PiiGAB M-Bus SoftwarePack 900S does not correctly sanitize user input, which could allow an attacker to inject arbitrary commands. **CVE ID : CVE-2023-36859**	N/A	O-PII-M-BU-250723/4730
Cross-Site Request Forgery (CSRF)	07-Jul-2023	8.8	PiiGAB M-Bus is vulnerable to cross-site request forgery. An attacker who wants to execute a certain command could send a phishing mail to the owner of the device and hope that the	N/A	O-PII-M-BU-250723/4731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			owner clicks on the link. If the owner of the device has a cookie stored that allows the owner to be logged in, then the device could execute the GET or POST link request. **CVE ID : CVE-2023-35120**		
Unprotected Transport of Credentials	06-Jul-2023	7.5	PiiGAB M-Bus transmits credentials in plaintext format. **CVE ID : CVE-2023-31277**	N/A	O-PII-M-BU-250723/4732
Unprotected Storage of Credentials	07-Jul-2023	6.5		N/A	O-PII-M-BU-250723/4733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PiiGAB M-Bus stores credentials in a plaintext file, which could allow a low-level user to gain admin credentials. **CVE ID : CVE-2023-35765**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-2023	6.1	PiiGAB M-Bus does not validate identification strings before processing, which could make it vulnerable to cross-site scripting attacks.	N/A	O-PII-M-BU-250723/4734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32652		
Vendor: Qualcomm					
Product: 205_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-205_-250723/4735
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-205_-250723/4736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-205_-250723/4737
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-205_-250723/4738
Product: 215_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-215_-250723/4739
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-215_-250723/4740
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/company/product-security/bull	O-QUA-215_-250723/4741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	etins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-215_-250723/4742
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-215_-250723/4743
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-215_-250723/4744
Product: 315_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-315_-250723/4745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-315_-250723/4746
Product: 315_5g_iot_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-315_-250723/4747
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-315_-250723/4748
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-315_-250723/4749
Product: 9205_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE	https://www.qualcomm.com/company/product-security/bull	O-QUA-9205-250723/4750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security mode command message received from network. **CVE ID : CVE-2023-21631**	etins/july-2023-bulletin	
Product: apq8017_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-APQ8-250723/4751
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-APQ8-250723/4752
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-APQ8-250723/4753
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-APQ8-250723/4754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
Product: apq8037_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-APQ8-250723/4755
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-APQ8-250723/4756
Product: apq8064au_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-APQ8-250723/4757
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-APQ8-250723/4758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: aqt1000_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AQT1-250723/4759
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AQT1-250723/4760
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AQT1-250723/4761
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AQT1-250723/4762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AQT1-250723/4763
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AQT1-250723/4764
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AQT1-250723/4765
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AQT1-250723/4766
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AQT1-250723/4767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AQT1-250723/4768
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AQT1-250723/4769
Product: ar8031_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AR80-250723/4770
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AR80-250723/4771
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AR80-250723/4772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AR80-250723/4773
Product: ar8035_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AR80-250723/4774
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AR80-250723/4775
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AR80-250723/4776
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/company/product-security/bull	O-QUA-AR80-250723/4777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AR80-250723/4778
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AR80-250723/4779
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AR80-250723/4780
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AR80-250723/4781
Product: ar9380_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/compa	O-QUA-AR93-250723/4782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-AR93-250723/4783
Product: c-v2x_9150_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-C-V2-250723/4784
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-C-V2-250723/4785
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-C-V2-250723/4786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-C-V2-250723/4787
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-C-V2-250723/4788
Product: csr8811_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSR8-250723/4789
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSR8-250723/4790
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-CSR8-250723/4791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24851	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSR8-250723/4792
Product: csra6620_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRA-250723/4793
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRA-250723/4794
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRA-250723/4795
Integer Overflow	04-Jul-2023	7.8	Memory Corruption in Audio while	https://www.qualcomm	O-QUA-CSRA-250723/4796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	.com/company/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRA-250723/4797
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRA-250723/4798
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRA-250723/4799
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRA-250723/4800
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while	https://www.qualcomm.com/company/product-	O-QUA-CSRA-250723/4801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	security/bulletins/july-2023-bulletin	
Product: csra6640_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRA-250723/4802
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRA-250723/4803
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRA-250723/4804
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRA-250723/4805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRA-250723/4806
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRA-250723/4807
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRA-250723/4808
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRA-250723/4809
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRA-250723/4810
Product: csrb31024_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRB-250723/4811
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRB-250723/4812
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRB-250723/4813
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRB-250723/4814
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-CSRB-250723/4815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRB-250723/4816
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-CSRB-250723/4817
Product: fastconnect_6200_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4818
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4820
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4821
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4822
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4823
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4825
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4826
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4827
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4828
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4830
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4831
Product: fastconnect_6700_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4832
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4833
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/compa	O-QUA-FAST-250723/4834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	ny/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4835
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4836
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4837
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4838
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bull	O-QUA-FAST-250723/4839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4840
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4841
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4842
Product: fastconnect_6800_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4844
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4845
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4846
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4847
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4849
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4850
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4851
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4852
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4854
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4855
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4856
Product: fastconnect_6900_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4857
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsReg	https://www.qualcomm.com/company/product-security/bull	O-QUA-FAST-250723/4858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			isterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4859
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4860
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4861
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux when the file upload API is called with parameters having large buffer. **CVE ID : CVE-2023-21640**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4862
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause	https://www.qualcomm.com/company/product-security/bull	O-QUA-FAST-250723/4863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undesired system behavior. **CVE ID : CVE-2023-21641**	etins/july-2023-bulletin	
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4864
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4865
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4866
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4867
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/company/product-security/bull	O-QUA-FAST-250723/4868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4869
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4870
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4871
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4872
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-FAST-250723/4873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21624	2023-bulletin	
Product: fastconnect_7800_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4874
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4875
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux when the file upload API is called with parameters having large buffer. **CVE ID : CVE-2023-21640**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4876
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4878
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4879
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4880
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4881
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4883
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4884
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FAST-250723/4885
Product: flight_rb5_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FLIG-250723/4886
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FLIG-250723/4887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FLIG-250723/4888
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FLIG-250723/4889
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FLIG-250723/4890
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FLIG-250723/4891
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-FLIG-250723/4892
Product: home_hub_100_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-HOME-250723/4893
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-HOME-250723/4894
Product: immersive_home_214_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4895
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4896
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4898
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4899
Product: immersive_home_216_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4900
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4901
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4903
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4904
Product: immersive_home_316_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4905
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4906
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4908
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4909
Product: immersive_home_318_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4910
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4911
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4913
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IMME-250723/4914
Product: ipq4018_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ4-250723/4915
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ4-250723/4916
Product: ipq4019_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bull	O-QUA-IPQ4-250723/4917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ4-250723/4918
Product: ipq4028_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ4-250723/4919
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ4-250723/4920
Product: ipq4029_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ4-250723/4921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ4-250723/4922
Product: ipq5010_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ5-250723/4923
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ5-250723/4924
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ5-250723/4925
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ5-250723/4926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ5-250723/4927
Product: ipq5028_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ5-250723/4928
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ5-250723/4929
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ5-250723/4930
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ5-250723/4931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ipq6000_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ6-250723/4932
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ6-250723/4933
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ6-250723/4934
Product: ipq6010_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ6-250723/4935
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bull	O-QUA-IPQ6-250723/4936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ6-250723/4937
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ6-250723/4938
Product: ipq6018_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ6-250723/4939
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ6-250723/4940
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/company/product-security/bull	O-QUA-IPQ6-250723/4941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ6-250723/4942
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ6-250723/4943
Product: ipq6028_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ6-250723/4944
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ6-250723/4945
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/compa	O-QUA-IPQ6-250723/4946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ6-250723/4947
Product: ipq8064_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4948
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4949
Product: ipq8065_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4951
Product: ipq8068_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4952
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4953
Product: ipq8070a_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4954
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bull	O-QUA-IPQ8-250723/4955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4956
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4957
Product: ipq8070_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4958
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4959
Product: ipq8071a_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4960
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4961
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4962
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4963
Product: ipq8072a_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4965
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4966
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4967
Product: ipq8074a_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4968
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4970
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4971
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4972
Product: ipq8076a_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4973
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4975
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4976
Product: ipq8076_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4977
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4978
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4980
Product: ipq8078a_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4981
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4982
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4983
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ipq8078_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4985
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4986
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4987
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4988
Product: ipq8173_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	https://www.qualcomm.com/company/product-security/bull	O-QUA-IPQ8-250723/4989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22386	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4990
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4991
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4992
Product: ipq8174_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4993
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/company/product-security/bull	O-QUA-IPQ8-250723/4994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4995
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4996
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ8-250723/4997
Product: ipq9008_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ9-250723/4998
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/compa	O-QUA-IPQ9-250723/4999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ9-250723/5000
Product: ipq9574_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ9-250723/5001
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ9-250723/5002
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ9-250723/5003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-IPQ9-250723/5004
Product: mdm9250_firmware					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MDM9-250723/5005
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MDM9-250723/5006
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MDM9-250723/5007
Product: mdm9628_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE	https://www.qualcomm.com/company/product-security/bull	O-QUA-MDM9-250723/5008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security mode command message received from network. **CVE ID : CVE-2023-21631**	etins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MDM9-250723/5009
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MDM9-250723/5010
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MDM9-250723/5011
Product: mdm9640_firmware					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MDM9-250723/5012
Product: mdm9650_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MDM9-250723/5013
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MDM9-250723/5014
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MDM9-250723/5015
Product: msm8108_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MSM8-250723/5016
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/compa	O-QUA-MSM8-250723/5017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	ny/product-security/bulletins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MSM8-250723/5018
Product: msm8209_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MSM8-250723/5019
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MSM8-250723/5020
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-MSM8-250723/5021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: msm8608_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MSM8-250723/5022
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MSM8-250723/5023
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MSM8-250723/5024
Product: msm8909w_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MSM8-250723/5025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received from network. **CVE ID : CVE-2023-21631**		
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MSM8-250723/5026
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MSM8-250723/5027
Product: msm8996au_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MSM8-250723/5028
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-MSM8-250723/5029
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while	https://www.qualcomm.com/compa	O-QUA-MSM8-250723/5030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fetching TX status information. **CVE ID : CVE-2023-28542**	ny/product-security/bulletins/july-2023-bulletin	
Product: pmp8074_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-PMP8-250723/5031
Product: qam8255p_firmware					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5032
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5033
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QAM8-250723/5034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5035
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5036
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5037
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5038
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5040
Product: qam8295p_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5041
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5042
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5043
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QAM8-250723/5044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5045
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5046
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5047
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5048
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qam8650p_firmware					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5050
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5051
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5052
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5053
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QAM8-250723/5054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24854	2023-bulletin	
Product: qam8775p_firmware					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5055
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5056
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5057
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QAM8-250723/5058
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN	https://www.qualcomm.com/company/product-	O-QUA-QAM8-250723/5059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firmware response message. **CVE ID : CVE-2023-24854**	security/bulletins/july-2023-bulletin	
Product: qca4004_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA4-250723/5060
Product: qca4024_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA4-250723/5061
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA4-250723/5062
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA4-250723/5063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24851	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA4-250723/5064
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA4-250723/5065
Product: qca6174a_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5066
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5067
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM	https://www.qualcomm	O-QUA-QCA6-250723/5068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	.com/company/product-security/bulletins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5069
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5070
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5071
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5072
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-	O-QUA-QCA6-250723/5073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	security/bulletins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5074
Product: qca6175a_firmware					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5075
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5076
Product: qca6310_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5078
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5079
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5080
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5081
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5083
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5084
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5085
Product: qca6320_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5086
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5088
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5089
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5090
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5091
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5092
N/A	04-Jul-2023	5.5	Information disclosure in DSP	https://www.qualcomm	O-QUA-QCA6-250723/5093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Services while loading dynamic module. **CVE ID : CVE-2023-21624**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: qca6335_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5094
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5095
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5096
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5098
Product: qca6391_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5099
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5100
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5101
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs.	https://www.qualcomm.com/company/product-	O-QUA-QCA6-250723/5102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21637	security/bulletins/july-2023-bulletin	
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5103
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5104
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5105
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5106
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-250723/5107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24851	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5108
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5109
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5110
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5111
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca6420_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5113
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5114
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5115
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5116
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the	https://www.qualcomm.com/company/product-	O-QUA-QCA6-250723/5117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			one received in initialization. **CVE ID : CVE-2023-21638**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5118
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5119
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5120
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5121
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-250723/5122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	etins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5123
Product: qca6421_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5124
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5125
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5127
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5128
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5129
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5130
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5131
Product: qca6426_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5132
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5133
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5134
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5135
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-250723/5136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21638	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5137
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5138
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5139
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5140
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5142
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5143
Product: qca6430_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5144
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5145
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets	https://www.qualcomm.com/company/product-	O-QUA-QCA6-250723/5146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			detected on telephony. **CVE ID : CVE-2023-21635**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5147
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5148
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5149
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5150
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/company/product-	O-QUA-QCA6-250723/5151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5152
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5153
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5154
Product: qca6431_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5156
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5157
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5158
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5159
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5161
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5162
Product: qca6436_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5163
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5164
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets	https://www.qualcomm.com/company/product-	O-QUA-QCA6-250723/5165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			detected on telephony. **CVE ID : CVE-2023-21635**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5166
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5167
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5168
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5169
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-250723/5170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5171
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5172
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5173
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5174
Product: qca6554a_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-250723/5175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22386	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5176
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5177
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5178
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5179
Product: qca6564au_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-250723/5180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command message received from network. **CVE ID : CVE-2023-21631**	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5181
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5182
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5183
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5184
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/company/product-	O-QUA-QCA6-250723/5185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5186
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5187
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5188
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5189
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-250723/5190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
Product: qca6564a_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5191
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5192
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5193
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5195
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5196
Product: qca6564_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5197
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5198
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-250723/5199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5200
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5201
Product: qca6574au_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5202
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5204
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5205
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5206
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5207
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5209
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5210
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5211
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5212
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5214
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5215
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5216
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5217
Product: qca6574a_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received from network. **CVE ID : CVE-2023-21631**		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5219
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5220
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5221
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5222
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/company/product-	O-QUA-QCA6-250723/5223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5224
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5225
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5226
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5227
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-250723/5228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5229
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5230
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5231
Product: qca6574_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5232
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-250723/5233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5234
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5235
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5236
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5237
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-250723/5238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24854	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5239
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5240
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5241
Product: qca6584au_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5242
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-250723/5243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5244
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5245
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5246
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5247
Product: qca6584_firmware					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-250723/5248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	2023-bulletin	
Product: qca6595au_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5249
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5250
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5251
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5253
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5254
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5255
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5256
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5258
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5259
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5260
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5261
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5262
Product: qca6595_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5263
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5264
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5265
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5266
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5268
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5269
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5270
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5271
Product: qca6678aq_firmware					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca6696_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5273
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5274
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5275
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5276
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the	https://www.qualcomm.com/company/product-	O-QUA-QCA6-250723/5277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			one received in initialization. **CVE ID : CVE-2023-21638**	security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5278
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5279
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5280
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5281
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/company/product-	O-QUA-QCA6-250723/5282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5283
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5284
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5285
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5286
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-250723/5287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5288
Product: qca6698aq_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5289
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5290
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5292
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5293
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5294
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5295
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5297
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5298
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5299
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5300
Product: qca6797aq_firmware					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21672		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5302
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5303
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5304
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5305
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5307
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5308
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA6-250723/5309
Product: qca7500_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA7-250723/5310
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA7-250723/5311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca8072_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5312
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5313
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5314
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5315
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca8075_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5317
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5318
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5319
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5320
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca8081_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5322
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5323
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5324
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5325
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA8-250723/5326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firmware response message. **CVE ID : CVE-2023-24854**	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5327
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5328
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5329
Product: qca8082_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5330
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/compa	O-QUA-QCA8-250723/5331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5332
Product: qca8084_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5333
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5334
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5335
Product: qca8085_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5336
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5337
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5338
Product: qca8337_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5339
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA8-250723/5340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5341
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5342
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5343
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5344
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA8-250723/5345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5346
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5347
Product: qca8386_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5348
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA8-250723/5349
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA8-250723/5350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	2023-bulletin	
Product: qca9367_firmware					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5351
Product: qca9377_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5352
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5353
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5355
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5356
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5357
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5358
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5359
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to	https://www.qualcomm	O-QUA-QCA9-250723/5360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: qca9379_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5361
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5362
Product: qca9880_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5363
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA9-250723/5364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: qca9886_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5365
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5366
Product: qca9888_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5367
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5369
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5370
Product: qca9889_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5371
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5372
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5374
Product: qca9898_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5375
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5376
Product: qca9980_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5377
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA9-250723/5378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	etins/july-2023-bulletin	
Product: qca9984_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5379
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5380
Product: qca9985_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5381
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5382
Product: qca9986_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5383
Product: qca9990_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5384
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5385
Product: qca9992_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5386
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA	https://www.qualcomm.com/company/product-	O-QUA-QCA9-250723/5387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer release event about CFR data. **CVE ID : CVE-2023-28541**	security/bulletins/july-2023-bulletin	
Product: qca9994_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5388
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCA9-250723/5389
Product: qcm2290_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM2-250723/5390
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCM2-250723/5391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22386	2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM2-250723/5392
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM2-250723/5393
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM2-250723/5394
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM2-250723/5395
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM2-250723/5396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM2-250723/5397
Product: qcm4290_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM4-250723/5398
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM4-250723/5399
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM4-250723/5400
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCM4-250723/5401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM4-250723/5402
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM4-250723/5403
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM4-250723/5404
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM4-250723/5405
Product: qcm4325_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in	https://www.qualcomm.com/compa	O-QUA-QCM4-250723/5406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	ny/product-security/bulletins/july-2023-bulletin	
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM4-250723/5407
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM4-250723/5408
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM4-250723/5409
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM4-250723/5410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM4-250723/5411
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM4-250723/5412
Product: qcm4490_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM4-250723/5413
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM4-250723/5414
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCM4-250723/5415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM4-250723/5416
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM4-250723/5417
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM4-250723/5418
Product: qcm6125_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM6-250723/5419
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/compa	O-QUA-QCM6-250723/5420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM6-250723/5421
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM6-250723/5422
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM6-250723/5423
Product: qcm6490_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM6-250723/5424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21631		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM6-250723/5425
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM6-250723/5426
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM6-250723/5427
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM6-250723/5428
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM6-250723/5429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM6-250723/5430
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM6-250723/5431
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCM6-250723/5432
Product: qcn5021_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5433
Product: qcn5022_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN5-250723/5434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22386	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5435
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5436
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5437
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5438
Product: qcn5024_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN5-250723/5439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5440
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5441
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5442
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5443
Product: qcn5052_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/compa	O-QUA-QCN5-250723/5444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	ny/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5445
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5446
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5447
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5448
Product: qcn5054_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5449
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5450
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5451
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5452
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5453
Product: qcn5122_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5454
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5455
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5456
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5457
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5458
Product: qcn5124_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5459
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5460
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5461
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5462
Product: qcn5152_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5464
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5465
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5466
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5467
Product: qcn5154_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5469
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5470
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5471
Product: qcn5164_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5472
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5474
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN5-250723/5475
Product: qcn6023_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN6-250723/5476
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN6-250723/5477
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN6-250723/5478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN6-250723/5479
Product: qcn6024_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN6-250723/5480
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN6-250723/5481
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN6-250723/5482
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN6-250723/5483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN6-250723/5484
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN6-250723/5485
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN6-250723/5486
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN6-250723/5487
Product: qcn6100_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/compa	O-QUA-QCN6-250723/5488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	ny/product-security/bulletins/july-2023-bulletin	
Product: qcn6102_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN6-250723/5489
Product: qcn6112_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN6-250723/5490
Product: qcn6122_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN6-250723/5491
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN6-250723/5492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN6-250723/5493
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN6-250723/5494
Product: qcn6132_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN6-250723/5495
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN6-250723/5496
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN6-250723/5497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN6-250723/5498
Product: qcn7605_firmware					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN7-250723/5499
Product: qcn7606_firmware					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN7-250723/5500
Product: qcn9000_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCN9-250723/5501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22386	2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5502
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5503
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5504
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5505
Product: qcn9001_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCN9-250723/5506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22386	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5507
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5508
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5509
Product: qcn9002_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5510
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCN9-250723/5511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24851	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5512
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5513
Product: qcn9003_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5514
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5515
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCN9-250723/5516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24854	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5517
Product: qcn9011_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5518
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5519
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5520
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCN9-250723/5521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24851	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5522
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5523
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5524
Product: qcn9012_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5525
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCN9-250723/5526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5527
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5528
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5529
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5530
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcn9022_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5532
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5533
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5534
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5535
Product: qcn9024_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN9-250723/5536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security mode command message received from network. **CVE ID : CVE-2023-21631**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5537
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5538
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5539
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5540
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA	https://www.qualcomm.com/company/product-	O-QUA-QCN9-250723/5541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer release event about CFR data. **CVE ID : CVE-2023-28541**	security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5542
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5543
Product: qcn9070_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5544
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5545
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/compa	O-QUA-QCN9-250723/5546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5547
Product: qcn9072_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5548
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5549
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5551
Product: qcn9074_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5552
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5553
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5554
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5556
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5557
Product: qcn9100_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5558
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5559
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5561
Product: qcn9274_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5562
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5563
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5564
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCN9-250723/5565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcs2290_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS2-250723/5566
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS2-250723/5567
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS2-250723/5568
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS2-250723/5569
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCS2-250723/5570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS2-250723/5571
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS2-250723/5572
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS2-250723/5573
Product: qcs410_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS4-250723/5574
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/compa	O-QUA-QCS4-250723/5575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	ny/product-security/bulletins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS4-250723/5576
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS4-250723/5577
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS4-250723/5578
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS4-250723/5579
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCS4-250723/5580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	etins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS4-250723/5581
Product: qcs4290_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS4-250723/5582
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS4-250723/5583
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS4-250723/5584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS4-250723/5585
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS4-250723/5586
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS4-250723/5587
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS4-250723/5588
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS4-250723/5589
Product: qcs4490_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS4-250723/5590
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS4-250723/5591
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS4-250723/5592
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS4-250723/5593
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCS4-250723/5594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS4-250723/5595
Product: qcs610_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5596
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5597
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5598
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCS6-250723/5599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5600
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5601
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5602
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5603
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCS6-250723/5604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: qcs6125_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5605
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5606
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5607
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5608
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCS6-250723/5609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
Product: qcs6490_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5610
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5611
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5612
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5614
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5615
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5616
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5617
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS6-250723/5618
Product: qcs8155_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS8-250723/5619
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS8-250723/5620
Product: qcs8250_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS8-250723/5621
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS8-250723/5622
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS8-250723/5623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS8-250723/5624
Product: qcs8550_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS8-250723/5625
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QCS8-250723/5626
Product: qrb5165m_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QRB5-250723/5627
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM	https://www.qualcomm	O-QUA-QRB5-250723/5628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	.com/company/product-security/bulletins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QRB5-250723/5629
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QRB5-250723/5630
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QRB5-250723/5631
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QRB5-250723/5632
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-	O-QUA-QRB5-250723/5633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	security/bulletins/july-2023-bulletin	
Product: qrb5165n_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QRB5-250723/5634
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QRB5-250723/5635
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QRB5-250723/5636
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QRB5-250723/5637
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN	https://www.qualcomm.com/company/product-	O-QUA-QRB5-250723/5638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firmware response message. **CVE ID : CVE-2023-24854**	security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QRB5-250723/5639
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QRB5-250723/5640
Product: qsm8250_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QSM8-250723/5641
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QSM8-250723/5642
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/compa	O-QUA-QSM8-250723/5643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	ny/product-security/bulletins/july-2023-bulletin	
Product: qsm8350_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QSM8-250723/5644
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QSM8-250723/5645
Product: qts110_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-QTS1-250723/5646
Product: robotics_rb3_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM	https://www.qualcomm	O-QUA-ROBO-250723/5647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	.com/company/product-security/bulletins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-ROBO-250723/5648
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-ROBO-250723/5649
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-ROBO-250723/5650
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-ROBO-250723/5651
Product: robotics_rb5_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-ROBO-250723/5652
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-ROBO-250723/5653
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-ROBO-250723/5654
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-ROBO-250723/5655
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-ROBO-250723/5656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-ROBO-250723/5657
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-ROBO-250723/5658
Product: sa4150p_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA41-250723/5659
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA41-250723/5660
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	https://www.qualcomm.com/company/product-security/bull	O-QUA-SA41-250723/5661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22386	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA41-250723/5662
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA41-250723/5663
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA41-250723/5664
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA41-250723/5665
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SA41-250723/5666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: sa4155p_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA41-250723/5667
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA41-250723/5668
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA41-250723/5669
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA41-250723/5670
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/compa	O-QUA-SA41-250723/5671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA41-250723/5672
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA41-250723/5673
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA41-250723/5674
Product: sa6145p_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5676
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5677
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5678
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5679
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5681
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5682
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5683
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5684
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5686
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5687
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5688
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5689
Product: sa6150p_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21633		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5691
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5692
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5693
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5694
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SA61-250723/5695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21672	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5696
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5697
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5698
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5699
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5701
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5702
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5703
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5704
Product: sa6155p_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21633		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5706
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5707
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5708
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5709
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SA61-250723/5710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21641	2023-bulletin	
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5711
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5712
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5713
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5714
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SA61-250723/5715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24851	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5716
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5717
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5718
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5719
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sa6155_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5721
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5722
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5723
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5724
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SA61-250723/5725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA61-250723/5726
Product: sa8145p_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5727
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5728
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5729
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the	https://www.qualcomm.com/company/product-security/bull	O-QUA-SA81-250723/5730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			one received in initialization. **CVE ID : CVE-2023-21638**	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5731
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5732
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5733
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5734
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/company/product-	O-QUA-SA81-250723/5735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5736
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5737
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5738
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5739
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SA81-250723/5740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5741
Product: sa8150p_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5742
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5743
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5744
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the	https://www.qualcomm.com/company/product-security/bull	O-QUA-SA81-250723/5745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			one received in initialization. **CVE ID : CVE-2023-21638**	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5746
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5747
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5748
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5749
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/company/product-	O-QUA-SA81-250723/5750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5751
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5752
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5753
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5754
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SA81-250723/5755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5756
Product: sa8155p_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5757
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5758
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5759
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the	https://www.qualcomm.com/company/product-security/bull	O-QUA-SA81-250723/5760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			one received in initialization. **CVE ID : CVE-2023-21638**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5761
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5762
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5763
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5764
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/compa	O-QUA-SA81-250723/5765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	ny/product-security/bulletins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5766
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5767
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5768
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5769
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bull	O-QUA-SA81-250723/5770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	etins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5771
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5772
Product: sa8155_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5773
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5774
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/company/product-	O-QUA-SA81-250723/5775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5776
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5777
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5778
Product: sa8195p_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5779
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity	https://www.qualcomm.com/compa	O-QUA-SA81-250723/5780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5781
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5782
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5783
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5784
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent	https://www.qualcomm.com/compa	O-QUA-SA81-250723/5785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5786
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5787
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5788
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5789
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN	https://www.qualcomm.com/company/product-	O-QUA-SA81-250723/5790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firmware response message. **CVE ID : CVE-2023-24854**	security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5791
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5792
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5793
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA81-250723/5794
Product: sa8255p_firmware					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent	https://www.qualcomm.com/compa	O-QUA-SA82-250723/5795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA82-250723/5796
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA82-250723/5797
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA82-250723/5798
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA82-250723/5799
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN	https://www.qualcomm.com/company/product-	O-QUA-SA82-250723/5800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firmware response message. **CVE ID : CVE-2023-24854**	security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA82-250723/5801
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA82-250723/5802
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA82-250723/5803
Product: sa8295p_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA82-250723/5804
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent	https://www.qualcomm.com/compa	O-QUA-SA82-250723/5805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA82-250723/5806
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA82-250723/5807
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA82-250723/5808
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA82-250723/5809
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN	https://www.qualcomm.com/company/product-	O-QUA-SA82-250723/5810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firmware response message. **CVE ID : CVE-2023-24854**	security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA82-250723/5811
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SA82-250723/5812
Product: sc8180x-aaab_firmware					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SC81-250723/5813
Product: sc8180x-aa_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SC81-250723/5814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21631		
Product: sc8180x-ab_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SC81-250723/5815
Product: sc8180x-acaf_firmware					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SC81-250723/5816
Product: sc8180x-ac_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SC81-250723/5817
Product: sc8180x-ad_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SC81-250723/5818
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SC81-250723/5819
Product: sc8180x-af_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SC81-250723/5820
Product: sc8180xp-aaab_firmware					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SC81-250723/5821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
Product: sc8180xp-aa_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SC81-250723/5822
Product: sc8180xp-ab_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SC81-250723/5823
Product: sc8180xp-acaf_firmware					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SC81-250723/5824
Product: sc8180xp-ac_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SC81-250723/5825
Product: sc8180xp-ad_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SC81-250723/5826
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SC81-250723/5827
Product: sc8180xp-af_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SC81-250723/5828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command message received from network. **CVE ID : CVE-2023-21631**	2023-bulletin	
Product: sc8180x\+sdx55_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SC81-250723/5829
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SC81-250723/5830
Product: sd460_firmware					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD46-250723/5831
Product: sd626_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD62-250723/5832
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD62-250723/5833
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD62-250723/5834
Product: sd660_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD66-250723/5835
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD66-250723/5836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD66-250723/5837
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD66-250723/5838
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD66-250723/5839
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD66-250723/5840
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SD66-250723/5841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD66-250723/5842
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD66-250723/5843
Product: sd662_firmware					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD66-250723/5844
Product: sd670_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD67-250723/5845
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM	https://www.qualcomm	O-QUA-SD67-250723/5846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	.com/company/product-security/bulletins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD67-250723/5847
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD67-250723/5848
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD67-250723/5849
Product: sd675_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD67-250723/5850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD67-250723/5851
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD67-250723/5852
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD67-250723/5853
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD67-250723/5854
Product: sd730_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD73-250723/5855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21633		
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD73-250723/5856
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD73-250723/5857
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD73-250723/5858
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD73-250723/5859
Product: sd820_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SD82-250723/5860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	2023-bulletin	
Product: sd821_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD82-250723/5861
Product: sd835_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD83-250723/5862
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD83-250723/5863
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD83-250723/5864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD83-250723/5865
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD83-250723/5866
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD83-250723/5867
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD83-250723/5868
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD83-250723/5869
N/A	04-Jul-2023	5.5	Information disclosure in DSP	https://www.qualcomm	O-QUA-SD83-250723/5870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Services while loading dynamic module. **CVE ID : CVE-2023-21624**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: sd855_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD85-250723/5871
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD85-250723/5872
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD85-250723/5873
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SD85-250723/5874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21637	2023-bulletin	
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD85-250723/5875
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD85-250723/5876
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD85-250723/5877
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD85-250723/5878
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SD85-250723/5879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD85-250723/5880
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD85-250723/5881
Product: sd865_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD86-250723/5882
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD86-250723/5883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD86-250723/5884
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD86-250723/5885
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD86-250723/5886
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD86-250723/5887
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD86-250723/5888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD86-250723/5889
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD86-250723/5890
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD86-250723/5891
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD86-250723/5892
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD86-250723/5893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD86-250723/5894
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD86-250723/5895
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD86-250723/5896
Product: sd888_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD88-250723/5897
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD88-250723/5898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD88-250723/5899
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD88-250723/5900
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD88-250723/5901
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD88-250723/5902
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SD88-250723/5903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD88-250723/5904
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD88-250723/5905
Product: sdm429w_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SDM4-250723/5906
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SDM4-250723/5907
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SDM4-250723/5908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	2023-bulletin	
Product: sdx20m_firmware					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SDX2-250723/5909
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SDX2-250723/5910
Product: sdx55_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SDX5-250723/5911
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SDX5-250723/5912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21633		
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SDX5-250723/5913
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SDX5-250723/5914
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SDX5-250723/5915
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SDX5-250723/5916
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SDX5-250723/5917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SDX5-250723/5918
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SDX5-250723/5919
Product: sdx57m_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SDX5-250723/5920
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SDX5-250723/5921
Product: sdx65m_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SDX6-250723/5922
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SDX6-250723/5923
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SDX6-250723/5924
Product: sd_455_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD_4-250723/5925
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD_4-250723/5926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	etins/july-2023-bulletin	
Product: sd_675_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD_6-250723/5927
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD_6-250723/5928
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD_6-250723/5929
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD_6-250723/5930
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while	https://www.qualcomm.com/compa	O-QUA-SD_6-250723/5931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	ny/product-security/bulletins/july-2023-bulletin	
Product: sd_8_gen1_5g_firmware					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD_8-250723/5932
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD_8-250723/5933
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD_8-250723/5934
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD_8-250723/5935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD_8-250723/5936
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD_8-250723/5937
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SD_8-250723/5938
Product: sg4150p_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SG41-250723/5939
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent	https://www.qualcomm.com/company/product-security/bull	O-QUA-SG41-250723/5940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SG41-250723/5941
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SG41-250723/5942
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SG41-250723/5943
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SG41-250723/5944
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SG41-250723/5945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
Product: sm4125_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM41-250723/5946
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM41-250723/5947
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM41-250723/5948
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM41-250723/5949
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SM41-250723/5950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	2023-bulletin	
Product: sm6250p_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM62-250723/5951
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM62-250723/5952
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM62-250723/5953
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM62-250723/5954
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bull	O-QUA-SM62-250723/5955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	etins/july-2023-bulletin	
Product: sm6250_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM62-250723/5956
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM62-250723/5957
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM62-250723/5958
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM62-250723/5959
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while	https://www.qualcomm.com/company/product-	O-QUA-SM62-250723/5960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	security/bulletins/july-2023-bulletin	
Product: sm7250p_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM72-250723/5961
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM72-250723/5962
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM72-250723/5963
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM72-250723/5964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM72-250723/5965
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM72-250723/5966
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM72-250723/5967
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM72-250723/5968
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM72-250723/5969
Product: sm7315_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM73-250723/5970
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM73-250723/5971
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM73-250723/5972
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM73-250723/5973
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SM73-250723/5974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM73-250723/5975
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM73-250723/5976
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM73-250723/5977
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM73-250723/5978
Product: sm7325p_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SM73-250723/5979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command message received from network. **CVE ID : CVE-2023-21631**	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM73-250723/5980
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM73-250723/5981
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM73-250723/5982
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM73-250723/5983
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	https://www.qualcomm.com/company/product-security/bull	O-QUA-SM73-250723/5984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24854	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM73-250723/5985
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM73-250723/5986
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SM73-250723/5987
Product: smart_audio_200_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SMAR-250723/5988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SMAR-250723/5989
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SMAR-250723/5990
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SMAR-250723/5991
Product: smart_audio_400_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SMAR-250723/5992
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/company/product-security/bull	O-QUA-SMAR-250723/5993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SMAR-250723/5994
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SMAR-250723/5995
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SMAR-250723/5996
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SMAR-250723/5997
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SMAR-250723/5998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SMAR-250723/5999
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SMAR-250723/6000
Product: smart_display_200_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SMAR-250723/6001
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SMAR-250723/6002
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SMAR-250723/6003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
Product: snapdragon_208_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6004
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6005
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6006
Product: snapdragon_210_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received from network. **CVE ID : CVE-2023-21631**		
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6008
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6009
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6010
Product: snapdragon_212_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6012
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6013
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6014
Product: snapdragon_425_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6015
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/company/product-security/bull	O-QUA-SNAP-250723/6016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	etins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6017
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6018
Product: snapdragon_427_firmware					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6019
Product: snapdragon_429_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21631		
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6021
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6022
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6023
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6024
Product: snapdragon_430_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command message received from network. **CVE ID : CVE-2023-21631**	2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6026
Product: snapdragon_435_firmware					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6027
Product: snapdragon_439_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6028
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/company/product-security/bull	O-QUA-SNAP-250723/6029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6030
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6031
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6032
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6033
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
Product: snapdragon_450_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6035
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6036
Product: snapdragon_460_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6037
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6039
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6040
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6041
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6042
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6043
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to	https://www.qualcomm	O-QUA-SNAP-250723/6044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: snapdragon_480\+_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6045
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6046
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6047
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6049
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6050
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6051
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6052
Product: snapdragon_480_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command message received from network. **CVE ID : CVE-2023-21631**	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6054
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6055
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6056
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6057
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	https://www.qualcomm.com/company/product-security/bull	O-QUA-SNAP-250723/6058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24854	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6059
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6060
Product: snapdragon_4_gen_1_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6061
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6063
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6064
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6065
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6066
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6067
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to	https://www.qualcomm	O-QUA-SNAP-250723/6068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: snapdragon_4_gen_2_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6069
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6070
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6071
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bull	O-QUA-SNAP-250723/6072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	etins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6073
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6074
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6075
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6076
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: snapdragon_625_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6078
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6079
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6080
Product: snapdragon_626_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6081
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/compa	O-QUA-SNAP-250723/6082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	ny/product-security/bulletins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6083
Product: snapdragon_630_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6084
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6085
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6087
Product: snapdragon_632_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6088
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6089
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6090
Product: snapdragon_636_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in	https://www.qualcomm.com/compa	O-QUA-SNAP-250723/6091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	ny/product-security/bulletins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6092
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6093
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6094
Product: snapdragon_660_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received from network. **CVE ID : CVE-2023-21631**	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6096
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6097
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6098
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6099
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24854	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6101
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6102
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6103
Product: snapdragon_662_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6105
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6106
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6107
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6108
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6109
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to	https://www.qualcomm	O-QUA-SNAP-250723/6110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: snapdragon_665_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6111
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6112
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6113
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28541	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6115
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6116
Product: snapdragon_670_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6117
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6118
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bull	O-QUA-SNAP-250723/6119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6120
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6121
Product: snapdragon_675_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6122
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6123
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/company/product-	O-QUA-SNAP-250723/6124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6125
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6126
Product: snapdragon_678_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6127
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6128
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/compa	O-QUA-SNAP-250723/6129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6130
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6131
Product: snapdragon_680_4g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6132
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21672	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6134
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6135
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6136
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6137
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6139
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6140
Product: snapdragon_685_4g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6141
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6142
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/compa	O-QUA-SNAP-250723/6143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	ny/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6144
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6145
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6146
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6147
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bull	O-QUA-SNAP-250723/6148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	etins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6149
Product: snapdragon_690_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6150
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6151
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6153
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6154
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6155
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6156
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6157
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to	https://www.qualcomm	O-QUA-SNAP-250723/6158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: snapdragon_695_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6159
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6160
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6161
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6163
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6164
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6165
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6166
Product: snapdragon_710_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsReg	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			isterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6168
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6169
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6170
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6171
Product: snapdragon_712_firmware					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while	https://www.qualcomm.com/compa	O-QUA-SNAP-250723/6172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	ny/product-security/bulletins/july-2023-bulletin	
Product: snapdragon_720g_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6173
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6174
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6175
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6176
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to	https://www.qualcomm	O-QUA-SNAP-250723/6177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: snapdragon_730g_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6178
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6179
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6180
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6182
Product: snapdragon_730_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6183
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6184
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6185
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6187
Product: snapdragon_732g_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6188
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6189
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6190
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bull	O-QUA-SNAP-250723/6191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	etins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6192
Product: snapdragon_750g_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6193
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6194
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6196
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6197
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6198
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6199
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6200
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to	https://www.qualcomm	O-QUA-SNAP-250723/6201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: snapdragon_765g_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6202
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6203
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6204
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6206
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6207
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6208
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6209
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_765_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6211
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6212
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6213
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6214
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/company/product-	O-QUA-SNAP-250723/6215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6216
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6217
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6218
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6219
Product: snapdragon_768g_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in	https://www.qualcomm.com/compa	O-QUA-SNAP-250723/6220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6221
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6222
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6223
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6225
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6226
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6227
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6228
Product: snapdragon_778g\+_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received from network. **CVE ID : CVE-2023-21631**		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6230
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6231
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6232
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6233
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24854	2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6235
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6236
Product: snapdragon_778g\+_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6237
Product: snapdragon_778g_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6239
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6240
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6241
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6242
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6244
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6245
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6246
Product: snapdragon_780g_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6247
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN	https://www.qualcomm.com/company/product-security/bull	O-QUA-SNAP-250723/6248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW request to allocate memory. **CVE ID : CVE-2023-22386**	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6249
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6250
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6251
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6252
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6254
Product: snapdragon_780g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6255
Product: snapdragon_782g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6256
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6258
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6259
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6260
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6261
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6262
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to	https://www.qualcomm	O-QUA-SNAP-250723/6263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	.com/company/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6264
Product: snapdragon_7c\+_gen_3_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6265
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6266
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6268
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6269
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6270
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6271
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6273
Product: snapdragon_7c_firmware					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6274
Product: snapdragon_7c_gen_2_firmware					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6275
Product: snapdragon_820_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6276
Integer Overflow	04-Jul-2023	7.8	Memory Corruption in Audio while	https://www.qualcomm	O-QUA-SNAP-250723/6277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	.com/company/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6278
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6279
Product: snapdragon_821_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6280
Product: snapdragon_835_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6282
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6283
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6284
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6285
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6287
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6288
Product: snapdragon_845_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6289
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6290
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6292
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6293
Product: snapdragon_850_firmware					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6294
Product: snapdragon_855\+\/860_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6296
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6297
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6298
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6299
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6301
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6302
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6303
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6304
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6305
Product: snapdragon_855_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6306
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6307
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6308
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6309
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21638	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6311
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6312
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6313
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6314
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6316
Product: snapdragon_865\+_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6317
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6318
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6320
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6321
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6322
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6323
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6325
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6326
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6327
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6328
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6329
Product: snapdragon_865\+_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6330
Product: snapdragon_865_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6331
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6332
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6333
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs.	https://www.qualcomm.com/company/product-	O-QUA-SNAP-250723/6334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21637	security/bulletins/july-2023-bulletin	
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6335
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6336
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6337
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6338
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24851	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6340
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6341
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6342
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6343
Product: snapdragon_865_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21624	2023-bulletin	
Product: snapdragon_870_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6345
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6346
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6347
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6349
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6350
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6351
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6352
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6354
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6355
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6356
Product: snapdragon_870_5_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6357
Product: snapdragon_870_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module.	https://www.qualcomm.com/company/product-security/bull	O-QUA-SNAP-250723/6358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21624	etins/july-2023-bulletin	
Product: snapdragon_888\+_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6359
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6360
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6361
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6363
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6364
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6365
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6366
Product: snapdragon_888\+_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_888_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6368
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6369
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6370
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6371
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/company/product-security/bull	O-QUA-SNAP-250723/6372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6373
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6374
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6375
Product: snapdragon_888_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6376
Product: snapdragon_8\+_gen_1_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6377
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6378
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6379
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6380
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6382
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6383
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6384
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6385
Product: snapdragon_8_gen_1_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command message received from network. **CVE ID : CVE-2023-21631**	2023-bulletin	
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6387
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux when the file upload API is called with parameters having large buffer. **CVE ID : CVE-2023-21640**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6388
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6389
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6391
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6392
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6393
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6394
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6396
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6397
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6398
Product: snapdragon_ar2_gen_1_firmware					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6399
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22386	2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6401
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6402
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6403
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6404
Product: snapdragon_auto_4g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command message received from network. **CVE ID : CVE-2023-21631**	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6406
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6407
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6408
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6409
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bull	O-QUA-SNAP-250723/6410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	etins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6411
Product: snapdragon_auto_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6412
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6413
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6415
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6416
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6417
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6418
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6420
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6421
Product: snapdragon_w5\+_gen_1_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6422
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6423
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets	https://www.qualcomm.com/company/product-	O-QUA-SNAP-250723/6424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			detected on telephony. **CVE ID : CVE-2023-21635**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6425
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6426
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6427
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6428
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/compa	O-QUA-SNAP-250723/6429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6430
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6431
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6432
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6433
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bull	O-QUA-SNAP-250723/6434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	etins/july-2023-bulletin	
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6435
Product: snapdragon_wear_1300_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6436
Product: snapdragon_wear_2100_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6437
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA	https://www.qualcomm.com/company/product-	O-QUA-SNAP-250723/6438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer release event about CFR data. **CVE ID : CVE-2023-28541**	security/bulletins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6439
Product: snapdragon_wear_2500_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6440
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6441
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_wear_3100_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6443
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6444
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6445
Product: snapdragon_wear_4100\+_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6447
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6448
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6449
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6450
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6451
Product: snapdragon_x12_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6452
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6453
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6454
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6455
Product: snapdragon_x12_lte_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22386	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6457
Product: snapdragon_x20_firmware					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6458
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6459
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6460
Product: snapdragon_x24_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in	https://www.qualcomm.com/compa	O-QUA-SNAP-250723/6461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	ny/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6462
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6463
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6464
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6465
Product: snapdragon_x50_5g_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6466
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6467
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6468
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6469
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6471
Product: snapdragon_x55_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6472
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6473
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6475
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6476
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6477
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6478
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6480
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6481
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6482
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6483
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6484
N/A	04-Jul-2023	5.5	Information disclosure in DSP	https://www.qualcomm	O-QUA-SNAP-250723/6485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Services while loading dynamic module. **CVE ID : CVE-2023-21624**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: snapdragon_x5_firmware					
Affected Version(s): -					
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6486
Product: snapdragon_x65_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6487
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6488
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/company/product-	O-QUA-SNAP-250723/6489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6490
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6491
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6492
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6493
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
Product: snapdragon_x70_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6495
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6496
Product: snapdragon_xr1_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6497
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6499
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6500
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6501
Product: snapdragon_xr2\+_gen_1_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6502
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6504
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6505
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6506
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6507
Product: snapdragon_xr2_5g_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SNAP-250723/6508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command message received from network. **CVE ID : CVE-2023-21631**	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6509
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6510
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6511
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6512
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or	https://www.qualcomm.com/company/product-	O-QUA-SNAP-250723/6513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6514
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6515
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6516
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6517
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	https://www.qualcomm.com/company/product-security/bull	O-QUA-SNAP-250723/6518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24854	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6519
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6520
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6521
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SNAP-250723/6522
Product: ssg2115p_firmware					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent	https://www.qualcomm.com/company/product-security/bull	O-QUA-SSG2-250723/6523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SSG2-250723/6524
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SSG2-250723/6525
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SSG2-250723/6526
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SSG2-250723/6527
Product: ssg2125p_firmware					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent	https://www.qualcomm.com/compa	O-QUA-SSG2-250723/6528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SSG2-250723/6529
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SSG2-250723/6530
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SSG2-250723/6531
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SSG2-250723/6532
Product: sw5100p_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6533
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6534
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6535
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6536
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SW51-250723/6537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed by HIDL client. **CVE ID : CVE-2023-21639**	2023-bulletin	
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6538
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6539
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6540
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6541
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN	https://www.qualcomm.com/company/product-security/bull	O-QUA-SW51-250723/6542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firmware response message. **CVE ID : CVE-2023-24854**	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6543
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6544
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6545
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6546
Product: sw5100_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in	https://www.qualcomm.com/compa	O-QUA-SW51-250723/6547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6548
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6549
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6550
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6552
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6553
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6554
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6555
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6557
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6558
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6559
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SW51-250723/6560
Product: sxr1120_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR1-250723/6561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21633		
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR1-250723/6562
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR1-250723/6563
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR1-250723/6564
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR1-250723/6565
Product: sxr1230p_firmware					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SXR1-250723/6566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR1-250723/6567
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR1-250723/6568
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR1-250723/6569
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR1-250723/6570
Product: sxr2130_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in	https://www.qualcomm.com/compa	O-QUA-SXR2-250723/6571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR2-250723/6572
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR2-250723/6573
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR2-250723/6574
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR2-250723/6575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR2-250723/6576
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR2-250723/6577
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR2-250723/6578
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR2-250723/6579
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR2-250723/6580
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to	https://www.qualcomm	O-QUA-SXR2-250723/6581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	.com/company/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR2-250723/6582
Product: sxr2230p_firmware					
Affected Version(s): -					
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR2-250723/6583
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR2-250723/6584
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR2-250723/6585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR2-250723/6586
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-SXR2-250723/6587
Product: video_collaboration_vc1_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VIDE-250723/6588
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VIDE-250723/6589
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-VIDE-250723/6590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VIDE-250723/6591
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VIDE-250723/6592
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VIDE-250723/6593
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VIDE-250723/6594
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VIDE-250723/6595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VIDE-250723/6596
Product: video_collaboration_vc3_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VIDE-250723/6597
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VIDE-250723/6598
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VIDE-250723/6599
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in	https://www.qualcomm.com/company/product-	O-QUA-VIDE-250723/6600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	security/bulletins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VIDE-250723/6601
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VIDE-250723/6602
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VIDE-250723/6603
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VIDE-250723/6604
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-VIDE-250723/6605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VIDE-250723/6606
Product: video_collaboration_vc5_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VIDE-250723/6607
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VIDE-250723/6608
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VIDE-250723/6609
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-VIDE-250723/6610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	2023-bulletin	
Product: vision_intelligence_100_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VISI-250723/6611
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VISI-250723/6612
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VISI-250723/6613
Product: vision_intelligence_200_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VISI-250723/6614
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/compa	O-QUA-VISI-250723/6615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	ny/product-security/bulletins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VISI-250723/6616
Product: vision_intelligence_300_firmware					
Affected Version(s): -					
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VISI-250723/6617
Product: vision_intelligence_400_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VISI-250723/6618
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VISI-250723/6619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VISI-250723/6620
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VISI-250723/6621
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-VISI-250723/6622
Product: wcd9306_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6623
Product: wcd9326_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper	https://www.qualcomm	O-QUA-WCD9-250723/6624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	.com/company/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6625
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6626
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6627
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6629
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6630
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6631
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6632
Product: wcd9335_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received from network. **CVE ID : CVE-2023-21631**		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6634
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6635
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6636
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6637
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCD9-250723/6638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6639
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6640
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6641
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6642
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6644
Product: wcd9340_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6645
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6646
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6647
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCD9-250723/6648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6649
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6650
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6651
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6652
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCD9-250723/6653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6654
Product: wcd9341_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6655
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6656
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6658
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6659
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6660
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6661
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6663
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6664
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6665
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6666
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6667
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to	https://www.qualcomm	O-QUA-WCD9-250723/6668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	.com/company/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6669
Product: wcd9360_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6670
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6671
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCD9-250723/6672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6673
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6674
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6675
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6676
Product: wcd9370_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCD9-250723/6677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command message received from network. **CVE ID : CVE-2023-21631**	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6678
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6679
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6680
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6681
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/compa	O-QUA-WCD9-250723/6682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6683
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6684
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6685
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6686
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCD9-250723/6687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	etins/july-2023-bulletin	
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6688
Product: wcd9371_firmware					
Affected Version(s): -					
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6689
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6690
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6691
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-	O-QUA-WCD9-250723/6692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	security/bulletins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6693
Product: wcd9375_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6694
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6695
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21672		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6697
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6698
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6699
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6700
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6702
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6703
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6704
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6705
Product: wcd9380_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received from network. **CVE ID : CVE-2023-21631**		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6707
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6708
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6709
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6710
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux when the file upload API is called with	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCD9-250723/6711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameters having large buffer. **CVE ID : CVE-2023-21640**	etins/july-2023-bulletin	
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6712
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6713
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6714
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6715
Integer Overflow or	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion	https://www.qualcomm.com/company/product-	O-QUA-WCD9-250723/6716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			buffer during the music playback. **CVE ID : CVE-2023-22667**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6717
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6718
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6719
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6720
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCD9-250723/6721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21629	2023-bulletin	
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6722
Product: wcd9385_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6723
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6724
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6726
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6727
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6728
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6729
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6731
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6732
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6733
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCD9-250723/6734
Product: wcn3610_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received from network. **CVE ID : CVE-2023-21631**		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6736
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6737
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6738
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6739
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback.	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-250723/6740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22667	etins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6741
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6742
Product: wcn3615_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6743
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6745
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6746
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6747
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6748
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6749
Product: wcn3620_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6750
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6751
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6752
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6753
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCN3-250723/6754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: wcn3660b_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6755
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6756
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6757
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6759
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6760
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6761
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6762
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6763
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to	https://www.qualcomm	O-QUA-WCN3-250723/6764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	.com/company/product-security/bulletins/july-2023-bulletin	
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6765
Product: wcn3660_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6766
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6767
Product: wcn3680b_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCN3-250723/6768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received from network. **CVE ID : CVE-2023-21631**	2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6769
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6770
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6771
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6772
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-250723/6773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	etins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6774
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6775
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6776
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6777
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCN3-250723/6778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: wcn3680_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6779
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6780
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6781
Product: wcn3910_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6783
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6784
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6785
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6786
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6788
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6789
Product: wcn3950_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6790
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6791
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or	https://www.qualcomm.com/company/product-	O-QUA-WCN3-250723/6792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6793
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6794
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6795
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6796
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-250723/6797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24854	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6798
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6799
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6800
Product: wcn3980_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6802
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6803
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6804
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6805
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21672		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6807
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6808
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6809
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6810
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6812
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6813
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6814
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6815
Product: wcn3988_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received from network. **CVE ID : CVE-2023-21631**		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6817
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6818
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6819
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6820
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or	https://www.qualcomm.com/company/product-	O-QUA-WCN3-250723/6821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6822
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6823
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6824
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6825
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-250723/6826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24854	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6827
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6828
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6829
Product: wcn3990_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6831
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6832
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6833
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6834
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6836
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6837
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6838
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6839
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN3-250723/6840
N/A	04-Jul-2023	5.5	Information disclosure in DSP	https://www.qualcomm	O-QUA-WCN3-250723/6841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Services while loading dynamic module. **CVE ID : CVE-2023-21624**	.com/company/product-security/bulletins/july-2023-bulletin	
Product: wcn6740_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN6-250723/6842
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN6-250723/6843
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN6-250723/6844
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN6-250723/6845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22387	etins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN6-250723/6846
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN6-250723/6847
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN6-250723/6848
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN6-250723/6849
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCN6-250723/6850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WCN6-250723/6851
Product: wsa8810_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6852
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6853
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6855
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6856
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6857
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6858
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WSA8-250723/6859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6860
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6861
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6862
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6863
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6865
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6866
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6867
Product: wsa8815_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6868
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsReg	https://www.qualcomm.com/company/product-security/bull	O-QUA-WSA8-250723/6869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			isterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6870
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6871
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6872
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6873
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or	https://www.qualcomm.com/company/product-	O-QUA-WSA8-250723/6874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6875
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6876
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6877
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6878
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	https://www.qualcomm.com/company/product-security/bull	O-QUA-WSA8-250723/6879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24854	etins/july-2023-bulletin	
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6880
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6881
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6882
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6883
Product: wsa8830_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE	https://www.qualcomm.com/company/product-security/bull	O-QUA-WSA8-250723/6884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security mode command message received from network. **CVE ID : CVE-2023-21631**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6885
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony. **CVE ID : CVE-2023-21635**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6886
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6887
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6888
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing	https://www.qualcomm.com/compa	O-QUA-WSA8-250723/6889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	ny/product-security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux when the file upload API is called with parameters having large buffer. **CVE ID : CVE-2023-21640**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6890
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause undesired system behavior. **CVE ID : CVE-2023-21641**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6891
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6892
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6893
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM	https://www.qualcomm	O-QUA-WSA8-250723/6894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	.com/company/product-security/bulletins/july-2023-bulletin	
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6895
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6896
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6897
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6898
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information.	https://www.qualcomm.com/company/product-	O-QUA-WSA8-250723/6899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28542	security/bulletins/july-2023-bulletin	
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6900
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module. **CVE ID : CVE-2023-21624**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6901
Product: wsa8832_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6902
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions.	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21672		
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6904
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6905
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6906
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI response message from firmware. **CVE ID : CVE-2023-24851**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6907
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6909
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6910
Product: wsa8835_firmware					
Affected Version(s): -					
N/A	04-Jul-2023	9.8	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network. **CVE ID : CVE-2023-21631**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6911
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request. **CVE ID : CVE-2023-21633**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6912
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in Data Network Stack & Connectivity when sim gets	https://www.qualcomm.com/company/product-	O-QUA-WSA8-250723/6913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			detected on telephony. **CVE ID : CVE-2023-21635**	security/bulletins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux while calling system configuration APIs. **CVE ID : CVE-2023-21637**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6914
Incorrect Type Conversion or Cast	04-Jul-2023	7.8	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization. **CVE ID : CVE-2023-21638**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6915
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client. **CVE ID : CVE-2023-21639**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6916
Out-of-bounds Write	04-Jul-2023	7.8	Memory corruption in Linux when the file upload API is called with parameters having large buffer. **CVE ID : CVE-2023-21640**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6917
N/A	04-Jul-2023	7.8	An app with non-privileged access can change global system brightness and cause	https://www.qualcomm.com/company/product-	O-QUA-WSA8-250723/6918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undesired system behavior. **CVE ID : CVE-2023-21641**	security/bulletins/july-2023-bulletin	
Use After Free	04-Jul-2023	7.8	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions. **CVE ID : CVE-2023-21672**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6919
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory. **CVE ID : CVE-2023-22386**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6920
N/A	04-Jul-2023	7.8	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption. **CVE ID : CVE-2023-22387**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6921
Integer Overflow or Wraparound	04-Jul-2023	7.8	Memory Corruption in Audio while allocating the ion buffer during the music playback. **CVE ID : CVE-2023-22667**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6922
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI	https://www.qualcomm.com/company/product-security/bull	O-QUA-WSA8-250723/6923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response message from firmware. **CVE ID : CVE-2023-24851**	etins/july-2023-bulletin	
Out-of-bounds Write	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message. **CVE ID : CVE-2023-24854**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6924
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data. **CVE ID : CVE-2023-28541**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6925
Out-of-bounds Read	04-Jul-2023	7.8	Memory Corruption in WLAN HOST while fetching TX status information. **CVE ID : CVE-2023-28542**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6926
Double Free	04-Jul-2023	6.8	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files. **CVE ID : CVE-2023-21629**	https://www.qualcomm.com/company/product-security/bulletins/july-2023-bulletin	O-QUA-WSA8-250723/6927
N/A	04-Jul-2023	5.5	Information disclosure in DSP Services while loading dynamic module.	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WSA8-250723/6928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21624	2023-bulletin	
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 7.0					
Weak Password Requirements	05-Jul-2023	7.5	A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat discovered that, when FIPS mode was enabled, not all of the cryptographic modules in use were FIPS-validated. **CVE ID : CVE-2023-3089**	https://access.redhat.com/security/cve/CVE-2023-3089, https://bugzilla.redhat.com/show_bug.cgi?id=2212085	O-RED-ENTE-250723/6929
Affected Version(s): 8.0					
Weak Password Requirements	05-Jul-2023	7.5	A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat discovered that, when FIPS mode was enabled, not all of the cryptographic modules in use were FIPS-validated. **CVE ID : CVE-2023-3089**	https://access.redhat.com/security/cve/CVE-2023-3089, https://bugzilla.redhat.com/show_bug.cgi?id=2212085	O-RED-ENTE-250723/6930
Affected Version(s): 9.0					
Weak Password Requirements	05-Jul-2023	7.5	A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat discovered that, when FIPS mode was enabled, not all of	https://access.redhat.com/security/cve/CVE-2023-3089, https://bugzilla.redhat.com/show_bug	O-RED-ENTE-250723/6931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the cryptographic modules in use were FIPS-validated. **CVE ID : CVE-2023-3089**	.cgi?id=2212085	
Product: enterprise_linux_kernel-based_virtual_machine					
Affected Version(s): -					
N/A	04-Jul-2023	7.1	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where a guest OS may be able to control resources for which it is not authorized, which may lead to information disclosure and data tampering. **CVE ID : CVE-2023-25517**	https://nvidia.custhelp.com/app/answers/detail/a_id/5468	O-RED-ENTE-250723/6932
Vendor: Samsung					
Product: android					
Affected Version(s): 11.0					
Out-of-bounds Write	06-Jul-2023	7.8	Stack out of bound write vulnerability in CdmaSmsParser of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30644**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2023	7.8	Heap out of bound write vulnerability in IpcRxIncomingCBMsg of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30645**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6934
Out-of-bounds Write	06-Jul-2023	7.8	Heap out of bound write vulnerability in BroadcastSmsConfig of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30646**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6935
Out-of-bounds Write	06-Jul-2023	7.8	Heap out of bound write vulnerability in IpcRxUsimPhoneBookCapa of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30647**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6936
Out-of-bounds Write	06-Jul-2023	7.8	Heap out of bound write vulnerability in RmtUimNeedApdu of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30649**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2023	7.8	Out of bounds read and write in callrunTspCmd of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code. **CVE ID : CVE-2023-30650**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6938
Out-of-bounds Write	06-Jul-2023	7.8	Out of bounds read and write in callgetTspsysfs of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code. **CVE ID : CVE-2023-30651**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6939
Out-of-bounds Write	06-Jul-2023	7.8	Out of bounds read and write in callrunTspCmdNoRead of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code. **CVE ID : CVE-2023-30652**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6940
Out-of-bounds Write	06-Jul-2023	7.8	Out of bounds read and write in enableTspDevice of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code.	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30653		
Improper Input Validation	06-Jul-2023	7.8	Improper input validation vulnerability in SCEPProfile prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities. **CVE ID : CVE-2023-30655**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6942
Improper Input Validation	06-Jul-2023	7.8	Improper input validation vulnerability in LSOItemData prior to SMR Jul-2023 Release 1 allows attackers to launch certain activities. **CVE ID : CVE-2023-30656**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6943
Improper Input Validation	06-Jul-2023	7.8	Improper input validation vulnerability in EnhancedAttestationResult prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities. **CVE ID : CVE-2023-30657**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6944
Improper Input Validation	06-Jul-2023	7.8	Improper input validation vulnerability in OemPersonalizationSetLock in libsec-ril prior to SMR Jul-2023 Release 1 allows local	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to cause an Out-Of-Bounds write. **CVE ID : CVE-2023-30663**		
Improper Input Validation	06-Jul-2023	7.8	Improper input validation vulnerability in RegisteredMSISDN prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities. **CVE ID : CVE-2023-30664**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6946
Out-of-bounds Write	06-Jul-2023	7.8	Improper input validation vulnerability in DoOemImeiSetPreconfig in libsec-ril prior to SMR Jul-2023 Release 1 allows local attackers to cause an Out-Of-Bounds write. **CVE ID : CVE-2023-30666**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6947
Out-of-bounds Write	06-Jul-2023	7.8	Out-of-bounds Write in BuildOemSecureSimLockResponse of libsec-ril prior to SMR Jul-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30668**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2023	7.8	Out-of-bounds Write in DoOemFactorySendFactoryTestResult of libsec-ril prior to SMR Jul-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30669**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6949
Out-of-bounds Write	06-Jul-2023	7.8	Out-of-bounds Write in BuildIpcFactoryDeviceTestEvent of libsec-ril prior to SMR Jul-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30670**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6950
Missing Authentication for Critical Function	06-Jul-2023	7.1	Missing authentication vulnerability in Galaxy Themes Service prior to SMR Jul-2023 Release 1 allows local attackers to delete arbitrary non-preloaded applications. **CVE ID : CVE-2023-30643**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6951
Out-of-bounds Write	06-Jul-2023	5.5	Stack out-of-bounds write vulnerability in IpcRxImeiUpdateImeiNoti of RILD priro to SMR Jul-2023	https://security.samsungmobile.com/securityUpdate.smsb?yea	O-SAM-ANDR-250723/6952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Release 1 cause a denial of service on the system. **CVE ID : CVE-2023-30648**	r=2023&month=07	
Out-of-bounds Read	06-Jul-2023	4.4	Improper input validation vulnerability in OnOemServiceMode in libsec-ril prior to SMR Jul-2023 Release 1 allows local attackers to cause an Out-Of-Bounds read. **CVE ID : CVE-2023-30665**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6953
N/A	06-Jul-2023	3.3	Improper access control vulnerability in PersonaManagerService prior to SMR Jul-2023 Release 1 allows local attackers to change confiugration. **CVE ID : CVE-2023-30640**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6954
Affected Version(s): 12.0					
Out-of-bounds Write	06-Jul-2023	7.8	Stack out of bound write vulnerability in CdmaSmsParser of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30644**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2023	7.8	Heap out of bound write vulnerability in IpcRxIncomingCBMsg of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30645**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6956
Out-of-bounds Write	06-Jul-2023	7.8	Heap out of bound write vulnerability in BroadcastSmsConfig of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30646**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6957
Out-of-bounds Write	06-Jul-2023	7.8	Heap out of bound write vulnerability in IpcRxUsimPhoneBookCapa of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30647**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6958
Out-of-bounds Write	06-Jul-2023	7.8	Heap out of bound write vulnerability in RmtUimNeedApdu of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30649**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2023	7.8	Out of bounds read and write in callrunTspCmd of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code. **CVE ID : CVE-2023-30650**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6960
Out-of-bounds Write	06-Jul-2023	7.8	Out of bounds read and write in callgetTspsysfs of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code. **CVE ID : CVE-2023-30651**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6961
Out-of-bounds Write	06-Jul-2023	7.8	Out of bounds read and write in callrunTspCmdNoRead of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code. **CVE ID : CVE-2023-30652**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6962
Out-of-bounds Write	06-Jul-2023	7.8	Out of bounds read and write in enableTspDevice of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code.	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30653		
Improper Input Validation	06-Jul-2023	7.8	Improper input validation vulnerability in SCEPProfile prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities. **CVE ID : CVE-2023-30655**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6964
Improper Input Validation	06-Jul-2023	7.8	Improper input validation vulnerability in LSOItemData prior to SMR Jul-2023 Release 1 allows attackers to launch certain activities. **CVE ID : CVE-2023-30656**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6965
Improper Input Validation	06-Jul-2023	7.8	Improper input validation vulnerability in EnhancedAttestation Result prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities. **CVE ID : CVE-2023-30657**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6966
Improper Input Validation	06-Jul-2023	7.8	Improper input validation vulnerability in OemPersonalization SetLock in libsec-ril prior to SMR Jul-2023 Release 1 allows local	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to cause an Out-Of-Bounds write. **CVE ID : CVE-2023-30663**		
Improper Input Validation	06-Jul-2023	7.8	Improper input validation vulnerability in RegisteredMSISDN prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities. **CVE ID : CVE-2023-30664**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6968
Out-of-bounds Write	06-Jul-2023	7.8	Improper input validation vulnerability in DoOemImeiSetPreconfig in libsec-ril prior to SMR Jul-2023 Release 1 allows local attackers to cause an Out-Of-Bounds write. **CVE ID : CVE-2023-30666**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6969
Out-of-bounds Write	06-Jul-2023	7.8	Out-of-bounds Write in BuildOemSecureSimLockResponse of libsec-ril prior to SMR Jul-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30668**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2023	7.8	Out-of-bounds Write in DoOemFactorySendFactoryTestResult of libsec-ril prior to SMR Jul-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30669**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6971
Out-of-bounds Write	06-Jul-2023	7.8	Out-of-bounds Write in BuildIpcFactoryDeviceTestEvent of libsec-ril prior to SMR Jul-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30670**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6972
Missing Authentication for Critical Function	06-Jul-2023	7.1	Missing authentication vulnerability in Galaxy Themes Service prior to SMR Jul-2023 Release 1 allows local attackers to delete arbitrary non-preloaded applications. **CVE ID : CVE-2023-30643**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6973
Improper Privilege Management	06-Jul-2023	5.5	Improper privilege management vulnerability in Galaxy Themes Service prior to SMR	https://security.samsungmobile.com/securityUpdate.smsb?yea	O-SAM-ANDR-250723/6974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Jul-2023 Release 1 allows local attackers to call privilege function. **CVE ID : CVE-2023-30642**	r=2023&month=07	
Out-of-bounds Write	06-Jul-2023	5.5	Stack out-of-bounds write vulnerability in IpcRxImeiUpdateImeiNoti of RILD priro to SMR Jul-2023 Release 1 cause a denial of service on the system. **CVE ID : CVE-2023-30648**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6975
N/A	06-Jul-2023	5.5	Exposure of Sensitive Information vulnerability in getDefaultChipId in UwbAospAdapterService prior to SMR Jul-2023 Release 1 allows local attackers to access the UWB chipset Identifier. **CVE ID : CVE-2023-30660**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6976
N/A	06-Jul-2023	5.5	Exposure of Sensitive Information vulnerability in getChipInfos in UwbAospAdapterService prior to SMR Jul-2023 Release 1 allows local attackers to access the UWB chipset Identifier.	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30661		
N/A	06-Jul-2023	5.5	Exposure of Sensitive Information vulnerability in getChipIds in UwbAospAdapterService prior to SMR Jul-2023 Release 1 allows local attackers to access the UWB chipset Identifier. **CVE ID : CVE-2023-30662**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6978
N/A	06-Jul-2023	5.5	Logic error in package installation via adb command prior to SMR Jul-2023 Release 1 allows local attackers to downgrade installed application. **CVE ID : CVE-2023-30671**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6979
Out-of-bounds Read	06-Jul-2023	4.4	Improper input validation vulnerability in OnOemServiceMode in libsec-ril prior to SMR Jul-2023 Release 1 allows local attackers to cause an Out-Of-Bounds read. **CVE ID : CVE-2023-30665**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6980
N/A	06-Jul-2023	3.3	Improper access control vulnerability in	https://security.samsungmobile.com/	O-SAM-ANDR-250723/6981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PersonaManagerService prior to SMR Jul-2023 Release 1 allows local attackers to change confiugration. **CVE ID : CVE-2023-30640**	securityUpdate.smsb?year=2023&month=07	
Affected Version(s): 13.0					
Out-of-bounds Write	06-Jul-2023	7.8	Stack out of bound write vulnerability in CdmaSmsParser of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30644**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6982
Out-of-bounds Write	06-Jul-2023	7.8	Heap out of bound write vulnerability in IpcRxIncomingCBMsg of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30645**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6983
Out-of-bounds Write	06-Jul-2023	7.8	Heap out of bound write vulnerability in BroadcastSmsConfig of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30646**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jul-2023	7.8	Heap out of bound write vulnerability in IpcRxUsimPhoneBookCapa of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30647**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6985
Out-of-bounds Write	06-Jul-2023	7.8	Heap out of bound write vulnerability in RmtUimNeedApdu of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code. **CVE ID : CVE-2023-30649**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6986
Out-of-bounds Write	06-Jul-2023	7.8	Out of bounds read and write in callrunTspCmd of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code. **CVE ID : CVE-2023-30650**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6987
Out-of-bounds Write	06-Jul-2023	7.8	Out of bounds read and write in callgetTspsysfs of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code.	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30651		
Out-of-bounds Write	06-Jul-2023	7.8	Out of bounds read and write in callrunTspCmdNoRead of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code. **CVE ID : CVE-2023-30652**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6989
Out-of-bounds Write	06-Jul-2023	7.8	Out of bounds read and write in enableTspDevice of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code. **CVE ID : CVE-2023-30653**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6990
Improper Input Validation	06-Jul-2023	7.8	Improper input validation vulnerability in SCEPProfile prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities. **CVE ID : CVE-2023-30655**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6991
Improper Input Validation	06-Jul-2023	7.8	Improper input validation vulnerability in LSOItemData prior to SMR Jul-2023 Release 1 allows	https://security.samsungmobile.com/securityUpdate.smsb?yea	O-SAM-ANDR-250723/6992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to launch certain activities. **CVE ID : CVE-2023-30656**	r=2023&month=07	
Improper Input Validation	06-Jul-2023	7.8	Improper input validation vulnerability in EnhancedAttestation Result prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities. **CVE ID : CVE-2023-30657**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6993
Improper Input Validation	06-Jul-2023	7.8	Improper input validation vulnerability in DataProfile prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities. **CVE ID : CVE-2023-30658**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6994
Improper Input Validation	06-Jul-2023	7.8	Improper input validation vulnerability in Transaction prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities. **CVE ID : CVE-2023-30659**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6995
Improper Input Validation	06-Jul-2023	7.8	Improper input validation vulnerability in OemPersonalization	https://security.samsungmobile.com/securityUpd	O-SAM-ANDR-250723/6996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SetLock in libsec-ril prior to SMR Jul-2023 Release 1 allows local attackers to cause an Out-Of-Bounds write. **CVE ID : CVE-2023-30663**	ate.smsb?year=2023&month=07	
Improper Input Validation	06-Jul-2023	7.8	Improper input validation vulnerability in RegisteredMSISDN prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities. **CVE ID : CVE-2023-30664**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6997
Out-of-bounds Write	06-Jul-2023	7.8	Improper input validation vulnerability in DoOemImeiSetPreconfig in libsec-ril prior to SMR Jul-2023 Release 1 allows local attackers to cause an Out-Of-Bounds write. **CVE ID : CVE-2023-30666**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6998
Out-of-bounds Write	06-Jul-2023	7.8	Out-of-bounds Write in BuildOemSecureSimLockResponse of libsec-ril prior to SMR Jul-2023 Release 1 allows local attacker to execute arbitrary code.	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/6999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30668		
Out-of-bounds Write	06-Jul-2023	7.8	Out-of-bounds Write in DoOemFactorySendFactoryTestResult of libsec-ril prior to SMR Jul-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30669**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/7000
Out-of-bounds Write	06-Jul-2023	7.8	Out-of-bounds Write in BuildIpcFactoryDeviceTestEvent of libsec-ril prior to SMR Jul-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30670**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/7001
Missing Authentication for Critical Function	06-Jul-2023	7.1	Missing authentication vulnerability in Galaxy Themes Service prior to SMR Jul-2023 Release 1 allows local attackers to delete arbitrary non-preloaded applications. **CVE ID : CVE-2023-30643**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/7002
Improper Privilege	06-Jul-2023	5.5	Improper privilege management vulnerability in	https://security.samsungmobile.com/	O-SAM-ANDR-250723/7003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			Galaxy Themes Service prior to SMR Jul-2023 Release 1 allows local attackers to call privilege function. **CVE ID : CVE-2023-30642**	securityUpdate.smsb?year=2023&month=07	
Out-of-bounds Write	06-Jul-2023	5.5	Stack out-of-bounds write vulnerability in IpcRxImeiUpdateImeiNoti of RILD priro to SMR Jul-2023 Release 1 cause a denial of service on the system. **CVE ID : CVE-2023-30648**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/7004
N/A	06-Jul-2023	5.5	Exposure of Sensitive Information vulnerability in getDefaultChipId in UwbAospAdapterService prior to SMR Jul-2023 Release 1 allows local attackers to access the UWB chipset Identifier. **CVE ID : CVE-2023-30660**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/7005
N/A	06-Jul-2023	5.5	Exposure of Sensitive Information vulnerability in getChipInfos in UwbAospAdapterService prior to SMR Jul-2023 Release 1 allows local attackers to access	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/7006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the UWB chipset Identifier. **CVE ID : CVE-2023-30661**		
N/A	06-Jul-2023	5.5	Exposure of Sensitive Information vulnerability in getChipIds in UwbAospAdapterService prior to SMR Jul-2023 Release 1 allows local attackers to access the UWB chipset Identifier. **CVE ID : CVE-2023-30662**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/7007
N/A	06-Jul-2023	5.5	Logic error in package installation via adb command prior to SMR Jul-2023 Release 1 allows local attackers to downgrade installed application. **CVE ID : CVE-2023-30671**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/7008
Out-of-bounds Read	06-Jul-2023	4.4	Improper input validation vulnerability in OnOemServiceMode in libsec-ril prior to SMR Jul-2023 Release 1 allows local attackers to cause an Out-Of-Bounds read. **CVE ID : CVE-2023-30665**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/7009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Jul-2023	4.3	Improper access control vulnerability in Settings prior to SMR Jul-2023 Release 1 allows physical attacker to use restricted user profile to access device owner's google account data. **CVE ID : CVE-2023-30641**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/7010
N/A	06-Jul-2023	3.3	Improper access control vulnerability in PersonaManagerService prior to SMR Jul-2023 Release 1 allows local attackers to change confiugration. **CVE ID : CVE-2023-30640**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/7011
N/A	06-Jul-2023	3.3	Improper access control in Audio system service prior to SMR Jul-2023 Release 1 allows attacker to send broadcast with system privilege. **CVE ID : CVE-2023-30667**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=07	O-SAM-ANDR-250723/7012
Vendor: sealos					
Product: sealos					
Affected Version(s): * Up to (including) 4.2.0					
Missing Authorization	03-Jul-2023	8.1	Sealos is a Cloud Operating System designed for managing cloud-native applications.	N/A	O-SEA-SEAL-250723/7013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			In version 4.2.0 and prior, there is a permission flaw in the Sealos billing system, which allows users to control the recharge resource account `sealos[.]io/v1/Payment`, resulting in the ability to recharge any amount of 1 renminbi (RMB). The charging interface may expose resource information. The namespace of this custom resource would be user's control and may have permission to correct it. It is not clear whether a fix exists. **CVE ID : CVE-2023-36815**		
Vendor: Tenda					
Product: ac10_firmware					
Affected Version(s): 15.03.06.47					
Out-of-bounds Write	10-Jul-2023	9.8	Tenda AC1206 V15.03.06.23 and AC10 V15.03.06.47 were discovered to contain a stack overflow in the wpapsk_crypto parameter in the fromSetWirelessRepeat function. **CVE ID : CVE-2023-37710**	N/A	O-TEN-AC10-250723/7014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	10-Jul-2023	9.8	Tenda AC1206 V15.03.06.23 and AC10 V15.03.06.47 were discovered to contain a stack overflow in the deviceId parameter in the saveParentControlInfo function. **CVE ID : CVE-2023-37711**	N/A	O-TEN-AC10-250723/7015
Product: ac1206_firmware					
Affected Version(s): 15.03.06.23					
Out-of-bounds Write	10-Jul-2023	9.8	Tenda AC1206 V15.03.06.23 and AC10 V15.03.06.47 were discovered to contain a stack overflow in the wpapsk_crypto parameter in the fromSetWirelessRepeat function. **CVE ID : CVE-2023-37710**	N/A	O-TEN-AC12-250723/7016
Out-of-bounds Write	10-Jul-2023	9.8	Tenda AC1206 V15.03.06.23 and AC10 V15.03.06.47 were discovered to contain a stack overflow in the deviceId parameter in the saveParentControlInfo function. **CVE ID : CVE-2023-37711**	N/A	O-TEN-AC12-250723/7017
Out-of-bounds Write	10-Jul-2023	9.8	Tenda AC1206 V15.03.06.23, F1202 V1.2.0.20(408), and	N/A	O-TEN-AC12-250723/7018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FH1202 V1.2.0.20(408) were discovered to contain a stack overflow in the page parameter in the fromSetIpBind function. **CVE ID : CVE-2023-37712**		
Product: f1202_firmware					
Affected Version(s): 1.2.0.20\\(408\\)					
Out-of-bounds Write	10-Jul-2023	9.8	Tenda AC1206 V15.03.06.23, F1202 V1.2.0.20(408), and FH1202 V1.2.0.20(408) were discovered to contain a stack overflow in the page parameter in the fromSetIpBind function. **CVE ID : CVE-2023-37712**	N/A	O-TEN-F120-250723/7019
Product: fh1202_firmware					
Affected Version(s): 1.2.0.20\\(408\\)					
Out-of-bounds Write	10-Jul-2023	9.8	Tenda AC1206 V15.03.06.23, F1202 V1.2.0.20(408), and FH1202 V1.2.0.20(408) were discovered to contain a stack overflow in the page parameter in the fromSetIpBind function. **CVE ID : CVE-2023-37712**	N/A	O-TEN-FH12-250723/7020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: fh1203_firmware					
Affected Version(s): 2.0.1.6					
Out-of-bounds Write	10-Jul-2023	9.8	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the ssid parameter in the form_fast_setting_wifi_set function. **CVE ID : CVE-2023-37700**	N/A	O-TEN-FH12-250723/7021
Out-of-bounds Write	10-Jul-2023	9.8	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the deviceId parameter in the addWifiMacFilter function. **CVE ID : CVE-2023-37701**	N/A	O-TEN-FH12-250723/7022
Out-of-bounds Write	10-Jul-2023	9.8	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the deviceId parameter in the formSetDeviceName function. **CVE ID : CVE-2023-37702**	N/A	O-TEN-FH12-250723/7023
Out-of-bounds Write	10-Jul-2023	9.8	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the speed_dir parameter in the	N/A	O-TEN-FH12-250723/7024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			formSetSpeedWan function. **CVE ID : CVE-2023-37703**		
Out-of-bounds Write	10-Jul-2023	9.8	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function. **CVE ID : CVE-2023-37704**	N/A	O-TEN-FH12-250723/7025
Out-of-bounds Write	10-Jul-2023	9.8	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the page parameter in the fromAddressNat function. **CVE ID : CVE-2023-37705**	N/A	O-TEN-FH12-250723/7026
Out-of-bounds Write	10-Jul-2023	9.8	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the entrys parameter in the fromAddressNat function. **CVE ID : CVE-2023-37706**	N/A	O-TEN-FH12-250723/7027
Out-of-bounds Write	10-Jul-2023	9.8	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the page parameter in	N/A	O-TEN-FH12-250723/7028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the fromVirtualSer function. **CVE ID : CVE-2023-37707**		
Vendor: Tendacn					
Product: ac10_firmware					
Affected Version(s): 15.03.06.26					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jul-2023	9.8	Tenda AC10 v15.03.06.26 was discovered to contain a command injection vulnerability via the mac parameter in the function formWriteFacMac. **CVE ID : CVE-2023-37144**	N/A	O-TEN-AC10-250723/7029
Vendor: totolink					
Product: a3300r_firmware					
Affected Version(s): 17.0.0cu.557_b20221024					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-2023	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain an unauthenticated remote code execution (RCE) vulnerability via the lang parameter in the setLanguageCfg function. **CVE ID : CVE-2023-37170**	N/A	O-TOT-A330-250723/7030
Improper Neutralization of Special Elements	07-Jul-2023	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command	N/A	O-TOT-A330-250723/7031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			injection vulnerability via the admuser parameter in the setPasswordCfg function. **CVE ID : CVE-2023-37171**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-2023	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the ip parameter in the setDiagnosisCfg function. **CVE ID : CVE-2023-37172**	N/A	O-TOT-A330-250723/7032
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-2023	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the command parameter in the setTracerouteCfg function. **CVE ID : CVE-2023-37173**	N/A	O-TOT-A330-250723/7033
Product: lr350_firmware					
Affected Version(s): 9.3.5u.6369_b20220309					
Improper Neutralization of Special Elements used in a	07-Jul-2023	9.8	TOTOLINK LR350 V9.3.5u.6369_B20220309 was discovered to contain a command injection vulnerability via the	N/A	O-TOT-LR35-250723/7034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			hostname parameter in the setOpModeCfg function. **CVE ID : CVE-2023-37145**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jul-2023	9.8	TOTOLINK LR350 V9.3.5u.6369_B20220309 was discovered to contain a command injection vulnerability via the FileName parameter in the UploadFirmwareFile function. **CVE ID : CVE-2023-37146**	N/A	O-TOT-LR35-250723/7035
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jul-2023	9.8	TOTOLINK LR350 V9.3.5u.6369_B20220309 was discovered to contain a command injection vulnerability via the ussd parameter in the setUssd function. **CVE ID : CVE-2023-37148**	N/A	O-TOT-LR35-250723/7036
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jul-2023	9.8	TOTOLINK LR350 V9.3.5u.6369_B20220309 was discovered to contain a command injection vulnerability via the FileName parameter in the setUploadSetting function. **CVE ID : CVE-2023-37149**	N/A	O-TOT-LR35-250723/7037
Vendor: tyan					
Product: s5552\/s5552gm2nr_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 3.0.0					
Files or Directories Accessible to External Parties	05-Jul-2023	4.2	A CWE-552 "Files or Directories Accessible to External Parties" in the web interface of the Tyan S5552 BMC version 3.00 allows an unauthenticated remote attacker to retrieve the private key of the TLS certificate in use by the BMC via forced browsing. This can then be abused to perform Man-in-the-Middle (MitM) attacks against victims that access the web interface through HTTPS. **CVE ID : CVE-2023-2538**	N/A	O-TYA-S555-250723/7038
Product: s5552\/s5552gm4nr_firmware					
Affected Version(s): 3.0.0					
Files or Directories Accessible to External Parties	05-Jul-2023	4.2	A CWE-552 "Files or Directories Accessible to External Parties" in the web interface of the Tyan S5552 BMC version 3.00 allows an unauthenticated remote attacker to retrieve the private key of the TLS certificate in use by the BMC via forced browsing. This can then be abused to perform Man-in-the-	N/A	O-TYA-S555-250723/7039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Middle (MitM) attacks against victims that access the web interface through HTTPS. **CVE ID : CVE-2023-2538**		
Product: s5552\/s5552wgm4nr-ex_firmware					
Affected Version(s): 3.0.0					
Files or Directories Accessible to External Parties	05-Jul-2023	4.2	A CWE-552 "Files or Directories Accessible to External Parties" in the web interface of the Tyan S5552 BMC version 3.00 allows an unauthenticated remote attacker to retrieve the private key of the TLS certificate in use by the BMC via forced browsing. This can then be abused to perform Man-in-the-Middle (MitM) attacks against victims that access the web interface through HTTPS. **CVE ID : CVE-2023-2538**	N/A	O-TYA-S555-250723/7040
Product: s5552\/s5552wgm4nr_firmware					
Affected Version(s): 3.0.0					
Files or Directories Accessible to External Parties	05-Jul-2023	4.2	A CWE-552 "Files or Directories Accessible to External Parties" in the web interface of the Tyan S5552 BMC version 3.00 allows	N/A	O-TYA-S555-250723/7041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an unauthenticated remote attacker to retrieve the private key of the TLS certificate in use by the BMC via forced browsing. This can then be abused to perform Man-in-the-Middle (MitM) attacks against victims that access the web interface through HTTPS. **CVE ID : CVE-2023-2538**		
Vendor: ui					
Product: unifi_os					
Affected Version(s): 3.1					
N/A	01-Jul-2023	9	UniFi OS 3.1 introduces a misconfiguration on consoles running UniFi Network that allows users on a local network to access MongoDB. Applicable Cloud Keys that are both (1) running UniFi OS 3.1 and (2) hosting the UniFi Network application. "Applicable Cloud Keys" include the following: Cloud Key Gen2 and Cloud Key Gen2 Plus. **CVE ID : CVE-2023-31997**	N/A	O-UI-UNIF-250723/7042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Vmware					
Product: sd-wan_edge_firmware					
Affected Version(s): From (including) 4.5.0 Up to (excluding) 4.5.2					
Missing Authorization	06-Jul-2023	7.5	VMware SD-WAN (Edge) contains a bypass authentication vulnerability. An unauthenticated attacker can download the Diagnostic bundle of the application under VMware SD-WAN Management. **CVE ID : CVE-2023-20899**	https://www.vmware.com/security/advisories/VMSA-2023-0015.html	O-VMW-SD-W-250723/7043
Product: vsphere					
Affected Version(s): -					
N/A	04-Jul-2023	7.1	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where a guest OS may be able to control resources for which it is not authorized, which may lead to information disclosure and data tampering. **CVE ID : CVE-2023-25517**	https://nvidia.custhelp.com/app/answers/detail/a_id/5468	O-VMW-VSPH-250723/7044
Vendor: westerndigital					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: my_cloud_os					
Affected Version(s): From (including) 5.02.104 Up to (excluding) 5.26.202					
Authentication Bypass by Spoofing	01-Jul-2023	9.8	An authentication bypass issue via spoofing was discovered in the token-based authentication mechanism that could allow an attacker to carry out an impersonation attack. This issue affects My Cloud OS 5 devices: before 5.26.202. **CVE ID : CVE-2023-22814**	https://www.westerndigital.com/support/product-security/wdc-23006-my-cloud-firmware-version-5-26-202	O-WES-MY_C-250723/7045
Vendor: zephyrproject					
Product: zephyr					
Affected Version(s): * Up to (including) 3.2.0					
NULL Pointer Dereference	10-Jul-2023	7.5	A missing nullptr-check in handle_ra_input can cause a nullptr-deref. **CVE ID : CVE-2023-0359**	https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-c7fq-vqm6-v5pf	O-ZEP-ZEPH-250723/7046
Affected Version(s): * Up to (including) 3.3.0					
Out-of-bounds Write	10-Jul-2023	8	The bluetooth HCI host layer logic not clearing a global reference to a semaphore after synchronously sending HCI commands may allow a malicious HCI Controller to cause the use of a	https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-xvvm-8mcm-9cq3	O-ZEP-ZEPH-250723/7047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dangling reference in the host layer, leading to a crash (DoS) or potential RCE on the Host layer. **CVE ID : CVE-2023-1901**		